Mobile privacy and apps: investigating behavior and attitude

A cross-cultural study comparing US and German library and information science students

Dissertation

zur Erlangung des akademischen Grades

Doctor philosophiae
(Dr. phil.)

eingereicht

an der Philosophische Fakultät I
der Humboldt-Universität zu Berlin
Institut für Bibliotheks- und Informationswissenschaft

Stefanie Havelka

Die Präsidentin der Humboldt-Universität zu Berlin
Prof. Dr.-Ing. Dr. Sabine Kunst
Die Dekanin der Philosophischen Fakultät
Prof. Dr. Gabriele Metzler

Gutachter 1: Prof. Michael Seadle, PhD
Gutachter 2: Prof. Dr. Wolfram Horstmann

Datum der Einreichung: 26.2.2020
Datum der Promotion: 26.6.2020

Abstract

Mobile privacy and apps: investigating behavior and attitude

A cross-cultural study comparing US and German library and information science students

Stefanie Havelka, Humboldt-Universität zu Berlin, Germany

Apps and smartphones are used permanently and ubiquitously around the world. Main purposes are to communicate, retrieve information, locate places, and to be entertained. However, many users are often unaware of or indifferent to what types of personal data certain apps can access and what is possibly shared with the device manufacturer, app vendor, and third parties.

Some authors such as Moscato, Altschuller, and Moscato (2013) argue, "feelings toward, and perceptions of privacy are intricately tied to personal characteristics and cultural influence" (2013, 92). While "some authors predict that new technologies will make societies more and more similar. Technological modernization is an important force toward culture change, and it leads to partly similar developments in different societies…"(Hofstede 2011, 22).

This dissertation examines the role of culture, mobile privacy, apps, and user behavior and attitude. The core research question is:

> Are there differences in the mobile privacy behaviors and attitudes
> of American and German library and information science students?

Library and information science students were chosen as informants since a) privacy education is part of the curriculum in many information science departments, and b) current students grew up using mobile technologies. As such, they might have been exposed to mobile learning in their education.

The majority of previous scholarly research investigates mobile privacy using quantitative research methods. Qualitative research methods are still a bit underrepresented. This research addresses this perceived literature gap, as currently no ethnographic research focuses on exploring mobile privacy attitudes and behavior in a cross-cultural setting.

This dissertation uses ethnography as its research methodology since culture is at the heart of ethnography. Furthermore, ethnographers try to make sense of behavior, customs, and

attitudes of the culture they observe and research. This ethnographer aims to portray a thick narrative and transforms participants' mobile privacy attitude and behavior into a rich account.

The research design is comprised of semi-structured interviews, coupled with experiments and participant observations about mobile technology use. Fieldwork 1 was conducted in two different sites: Humboldt-Universität zu Berlin, Germany, and Rutgers, the State University of New Jersey, USA. Fieldwork 2 was conducted via an online video conferencing platform. The fieldwork allowed to compare privacy policy attitudes, mobile privacy setting behaviors, and location service behaviors. The fieldwork, which was carried out between 2017 and 2018, further allowed to assess whether the Facebook/Cambridge Analytica data privacy scandal and the new European privacy law had influenced student's mobile privacy behavior and attitude.

Findings are portrayed by showcasing two composite narratives and different themes for Fieldwork 1. Themes highlighted are (among others) privacy policy attitude and behavior, mobile privacy setting behavior, location service attitude, and behavior. Fieldwork 2 depicts the themes Facebook scandal, General Data Protection Regulation (GDPR), privacy protection, and privacy education. Fieldwork 1 and 2 also include mobile security as a topic, which albeit not part of the research question, transpired in the data analysis. Furthermore, both findings depict linguistic highlights to exemplify emotions, feelings, and non-verbal cues on mobile privacy.

Contrary to what some other researchers have conveyed and what this researcher predicted, the findings have revealed that there are nearly no cultural differences in mobile privacy behavior and attitude. Similar attitudes, such as mobile privacy complacency, mobile privacy learned-helplessness, and mobile privacy pragmatism, seem to impact German and American students equally.

The findings provide support for further research recommendations, and in conclusion, this researcher highlights three contributions this study makes to the scholarly literature.

Keywords: mobile privacy, behavior, attitude, apps, library science, information science, mobile privacy learned helplessness, mobile privacy complacency, mobile privacy pragmatism

Zusammenfassung

Mobile privacy and apps: investigating behavior and attitude
A cross-cultural study comparing US and German library and information science students

Stefanie Havelka, Humboldt-Universität zu Berlin, Deutschland

Weltweit werden Apps und Smartphones benützt, um zu kommunizieren, sich zu informieren und sich den Weg zeigen zu lassen sowie zur Unterhaltung usw. Viele Benutzer sind sich jedoch oft nicht bewusst oder im Klaren darüber, auf welche persönlichen Daten bestimmte Apps, die sie heruntergeladen haben, zugegriffen werden kann und welche Daten möglicherweise mit dem Gerätehersteller, dem Anbieter von Apps oder mit Dritten geteilt werden.

Einige Wissenschaftler wie Moscato, Altschuller und Moscato (2013, 92) argumentieren, die Art und Weise, wie man seine Privatsphäre fühlt und wahrnimmt, ist abhängig von den persönlichen Eigenschaften und dem kulturellen Einfluss auf das Individuum. Dem steht die Meinung anderer Wissenschaftler z. B. die von Hofstede (2011, 22) gegenüber, der voraussagt, dass aufgrund der neuen Technologien Gesellschaften sich immer ähnlicher würden bzw. in verschiedenen Gesellschaften ähnliche Entwicklungen und ein ähnlicher Kulturwandel stattfinden werde.

Diese Dissertation untersucht das Nutzerverhalten und die Einstellungen von Smartphone- und App-BenutzerInnen und welche Rolle die Kultur in Bezug auf mobile Privatsphäre spielt. Die zentrale Forschungsfrage lautet:

> Gibt es Unterschiede im Verhalten und in der Einstellung von amerikanischen und deutschen Studenten der Bibliotheks- und Informationswissenschaften in Bezug auf die mobile Privatsphäre?

Als Informanten wurden Studierende der Bibliotheks- und Informationswissenschaften requiriert, da a) der Unterricht über Datenschutz und Privatsphäre in vielen informationswissenschaftlichen Fakultäten Teil des Lehrplans ist und b) die derzeitigen Studierende mit mobilen Technologien aufgewachsen sind. Sowohl während des Studiums als auch in ihrem Privatleben hatten sie direkt oder indirekt permanent mit mobilem Lernen zu tun.

Bekanntermaßen untersucht ein Großteil der bisherigen wissenschaftlichen Forschung die mobile Privatsphäre mit Hilfe quantitativer Forschungsmethoden. Qualitative Forschungs-

methoden sind hingegen oft unterrepräsentiert. Die vorliegende Forschung schließt diese Forschungslücke. Denn im Mittelpunkt dieser Dissertation steht die ethnographische Forschung in einem interkulturellen Umfeld, die sich auf die Erforschung von Einstellungen und Verhaltensweisen in Bezug auf die mobile Privatsphäre konzentriert.

Diese Dissertation verwendet die Ethnographie als Forschungsmethodik, da Kultur im Mittelpunkt der Ethnographie steht. Bekanntermaßen versuchen Ethnographen, das Verhalten, die Bräuche und die Einstellungen der Kultur, die sie beobachten und erforschen, zu verstehen. Die Ethnographin dieser Studie hat die Methode der dichten Beschreibung gewählt, um die Einstellung und das Verhalten der zwanzig Studienteilnehmenden (aus Deutschland und den USA) in Bezug auf Privatsphäre beim Benutzen des Smartphones in allen Facetten aufzuzeigen.
Das Forschungsdesign besteht aus halb-strukturierten Interviews, gekoppelt mit Experimenten und Beobachtungen der Teilnehmer über die Nutzung mobiler Technologien. Die Feldforschung 1 wurde (in persona) an zwei verschiedenen Orten durchgeführt: an der *Humboldt-Universität zu Berlin*, Deutschland, und an der *Rutgers State University of New Jersey*, USA. Die Feldforschung 2 wurde (digital) über eine Online-Videokonferenzplattform durchgeführt.
Forschungsfragen in den beiden Feldforschungen waren unter anderem: Welche Einstellungen haben die Probanden zu Datenschutzrichtlinien? Wie verhalten sich die Studienteilnehmenden, wenn sie an ihrem Smartphone die mobile Privatsphäre einstellen? Wie verhalten sie sich, wenn es bei bestimmten Apps um die Standortbestimmung geht?

Die beiden Feldforschungen, die zwischen 2017 und 2018 durchgeführt wurden, ermöglichten es darüber hinaus zu beurteilen, ob der Facebook/Cambridge Analytica-Datenschutzskandal und das neue europäische Datenschutzgesetz das Verhalten und die Einstellung der Studenten in Bezug auf den mobilen Datenschutz beeinflusst haben.

Die Präsentation der Ergebnisse aus der Feldforschung 1 erfolgt durch eine "zusammengesetzte Beschreibung" von zwei Studienteilnehmenden (eine gängige Methode in der ethnographischen Forschung) sowie anhand von Themen, die für die Forschungsfrage dieser Studie interessant sind. Im Folgenden ein paar Beispiele aus der Themenliste: Die

Einstellung und das Verhalten in Bezug auf den Datenschutz und das Verhalten bei der Standortbestimmung sowie das Verhalten bei der Einstellung der mobilen Privatsphäre.

In der Feldforschung 2 stehen die Themen Facebook-Skandal, EU-Datenschutz-Grundverordnung (DSGVO), welche Instanzen sollten für den Datenschutz verantwortlich sein, und Datenschutzerziehung im Vordergrund.
Innerhalb der Feldforschungen 1 und 2 wird auch das Thema mobile Sicherheit thematisiert, welches zwar ursprünglich nicht Teil der Forschungsfrage war, aber während der Datenanalyse der Feldforschung unerwartet mehrmals auftauchte.
Darüber hinaus werden bei den Ergebnissen auch sprachliche Besonderheiten bzw. Highlights (z.B. starke emotionale sprachliche Ausdrücke oder nonverbale Zeichen) aufgezeigt, denn sie veranschaulichen auch die Einstellung der einzelnen Studienteilnehmenden zur mobilen Privatsphäre.

Im Gegensatz dazu, was bisher erforscht wurde und was die Autorin dieser vorliegenden Studie prognostizierte, kommt es zu folgenden Ergebnissen in dieser Studie: Bei den Probanden (egal aus welcher Kultur sie stammen) können fast keine kulturellen Unterschiede im Verhalten und in der Einstellung zur mobilen Privatsphäre festgestellt werden. Stattdessen werden in Bezug auf die mobile Privatsphäre ähnliche Einstellungen unter den Studienteilnehmenden festgestellt. Zum einen die Selbstzufriedenheit ("Ich habe alles im Griff."), zum anderen das Gefühl der Hilfslosigkeit ("Ich kann eh nichts ändern, die sind mächtiger als ich.") und schließlich Pragmatismus ("Ok, die Daten sind eh schon im Umlauf und ich brauche diese App eben.") scheinen, deutsche und amerikanische Studierende gleichermaßen zu beeinflussen. Das Ergebnis wurde aber ursprünglich nicht so erwartet, da eigentlich zu Beginn der Studie davon ausgegangen wurde, dass der unterschiedliche Kenntnis- und Bewusstseinsstand zur mobilen Privatsphäre in beiden Kulturen zu unterschiedlichen Reaktionen führen würde.

Dennoch bieten die Ergebnisse dieser Studie sicher nachfolgenden WissenschaftlerInnen interessante Impulse und eine gute Ausgangsbasis für weitere Studien.

Schlüsselwörter: Mobile Privatsphäre, Verhalten, Einstellung, Apps, Bibliothekswissenschaft, Informationswissenschaft, angelernte Hilflosigkeit, Selbstzufriedenheit, Pragmatismus

Dedication

"Here's to the crazy ones, the misfits, the rebels, the troublemakers, the round pegs in the square holes ... the ones who see things differently -- they're not fond of rules, and they have no respect for the status quo. ... You can quote them, disagree with them, glorify or vilify them, but the only thing you can't do is ignore them because they change things. ... They push the human race forward, and while some may see them as the crazy ones, we see genius, because the people who are crazy enough to think that they can change the world, are the ones who do.
— Steve Jobs, 1997

I dedicate this dissertation to my nieces Leonie, Anabel, Klara, Jana, and Ronja. And to my nephew Jonas. I wish for you to grow up in a world where mobile privacy still matters, where you allowed to keep secrets and decide what or what not to share with the digital world. Most of all, I want you to remember to turn off the phone and leave the online world behind. To cherish nature and animals, to enjoy spending time with friends, family, and strangers and to read a print book.

Not all the time, but at least some hours and days.

Acknowledgments

As usual, I write these words while most people are asleep. I like the night, the night is quiet, and I can focus on what matters to finish this doctoral thesis – research, reading, writing, and thinking. Writing this dissertation has been a long journey. Not only has it brought me to the end of the world and back, but it also has shown me that, all odds and obstacles aside, I have always had and still have a real passion for the topic of this dissertation – mobile privacy. And yes, I still love research and writing. It also has shown me that sometimes, no matter what, you have to continue, to walk your path, in order to find the answer or not.

First, I would like to thank my research participants: students from Germany and the US. Thank you. Dankeschön.

I could not have done it without the support, love, guidance, advice, and patience I received from the following people:

In Berlin, Germany:

At the Berlin School of Library and Information Science:

My doctoral advisor, or as they say in German Doktorvater, Prof. Dr. Michael Seadle. Thank you for guiding me, for calming my nerves and for all your support through the years. And yes, I still feel like a fried fish.

Prof. Dr. Wolfram Horstmann, my secondary reader. Thank you for your time and support. Danke.

Thanks to my fellow doctoral students for shared ideas and thoughts: Melanie Rügenhagen, Thomas Hartmann, Ulla Wimmer, Hossam El-Zalabany, and Johannes Neuer.
Thank you to Kirsten Schlebbe, Stefanie van den Sandt, and Celine Kaempf.
Stefanie Weissmann, administrative assistant, faculty of philosophy, for helping me through the maze of the administrative side of the doctorate. Thank you.

Jeff, Nicole, and Hailey Harwell - for your support, love, Kermit, chocolate, and friendship.
Esther Voelker, for your apartment, support, wise words, and love.

In Munich, Germany:

Dr. Sabine Dinsel – wow, just wow. Your support in the final few weeks made a huge, huge difference – thank you so much.

Dr. Uwe Junker – thanks for all your wise words and dinner invitations!

Mom and Dad – for food and taking care of Lucy – thank you. In Liebe und Dankbarkeit für Alles.

My sister Jasmin and her partner Manuel – thank you for everything. I love you both.

Julia Gickler, for your years of friendship and your extraordinary hospitality. I could not have finished it without you: love and gratitude. And to your boyfriend Michi – Danke.

In New York City, USA:

Katherine Lorimer, for your willingness to discuss the topic, to bounce off ideas and to proofread pages of pages. Love you always.

Jennifer King, for believing in me, every single day, for being a real and exceptional friend. My gratitude to you. Love you.

Dr. Devrim Yavuz, Lehman College, The City University of New York, for letting me hassle you with all my questions and always being supportive, thoughtful, and helpful. Merci beaucoup.

Devin Martin, who encouraged me to go for it.

John Rambow, for his editorial skills and proofreading and feedback. Thank you so much.

Martha Lerski, for sending me privacy articles over all these years and for a shared passion on the topic.

Stephen Walker at the Leonard Lief Library, Lehman College, The City University of New York. You have been always fast and super helpful.

Brendan McGibney, Lehman College, The City University of New York, for lending me the camcorder I used for recording the interviews.

Dr. Ted Taylor, Lehman College, The City University of New York, for proofreading and valuable feedback on the literature review chapter.

In Berkley, California USA

Colin Carlson, for reading and editing all my writing over all these years. Thank you. I am grateful to have you as my friend.

On Waiheke Island, New Zealand

Denny Reid – your daily support made all the difference. Thank you so much.

Bobby Lauper-Tisch and Leslie Hamilton. What a fun Mindmaster group we were. Thank you for coming through when I needed you most.

To the privacygrade.org: Thanks to the team of researchers, led by Professor Dr. Jason Hong, Carnegie Mellon University, primarily part of the CHIMPS lab.

And to all my **other friends in Germany and the USA** who continued to support and love me. I feel very blessed to have each of you in my life: Susan Coleman, Renate Oldoerp, Dorothee Burney, Freya Jeschke, Kerstin, and Matthias Rosmarion, Gayle Haring, Ulla Hofstaetter, Verena Henke, Jule Gruber, Sandra Doering, Sabine Keppelle, Stefanie Proessl, Veronika Hillebrandt, Marion Zeller, Kerstin Herzog, Jutta Gigl, Petra Schuster, Andreas Lowner, Don McConnell, Sven Wergandt, Robyn Schultz, Ulrike Schwerdtfeger, Katrin Elia, Rebecca and Danny Arzola, Helma Leuthe.

And to my partner Stefan Eisenmann: thanks for your love. I am glad you get me. You are my sunshine and happiness. Love you.

Lucy – for getting me out of the house, making me smile with her silly shenanigans, and for being the best dog ever. We will continue to have more adventures.

February 26, 2020
Stefanie Havelka

List of Figures

List of Tables

Abbreviations

AS 1-10	American Student 1-10
DM	Direct Message for Instagram
Fw1/2	Fieldwork 1/2
GDPR	General Date Protection Regulation
GPS	Global Positioning System
GS 1-10	German Student 1-10
iOS	Internet Operating System
iSchool	Information school organization
MAXQDA	Qualitative Data Analysis Software brand
mOS	mobile operating system
OS	Operating System
SC&I	School of Communication and Information at Rutgers University
SD-Card	Secure Digital Card
UAI	Uncertainty Avoidance

Table of Contents

1. Introduction

1.1 Mobile Devices, Apps, Privacy, and Libraries – an Entwined Mesh of Accessing, Tracking, Controlling, and Sharing Personal Information

When Steve Jobs, CEO of Apple, introduced the first iPhone on January 9, 2007 (McCormick 2017), little did we know that it would become such a game-changer for the smartphone market, information technology, and society as a whole (Molla 2017). Although the iPhone was not the first smartphone, Steve Job's vision of providing a computer in our pockets turned out to be seminal. Already in 2012, Saylor had stated that "mobile computing will be the most disruptive technology of our generation, and the revolution it leads is happening fast" (Saylor 2012, 37). This revolution has been unstoppable; predictions say that our global society will see an increase in smartphone penetration from 25% in 2011 to 36% in 2019 (*Number of Smartphone Users Worldwide 2014-2020*, 2019). In the United States 92% of adults aged 18-34 in 2015 versus 98% of the same age group owned a smartphone in 2018 (Taylor and Silver 2019, 5). In Germany the smartphone user penetration rate was 44.65% in 2014 versus a predicted 76.46% for 2020 (*Germany: Smartphone User Penetration 2015-2022*, 2020).

With the inroads that mobile devices made, mobile applications, better known as apps, became and remain immensely popular. "Apps emerged from early PDAs, through the addictively simple game Snake on the Nokia 6110 phone, to the first 500 apps in the Apple App Store, when it made its debut in July 2008" (Strain 2015, para. 5). Today there is a mind-boggling number of apps available: in the first quarter of 2018, Google Play and the Apple App Store offered 3.8 and 2 million different apps, respectively (*Number of Apps Available in Leading App Stores 2018 | Statistic* 2020). Apps are such a vital part of our information-technology- driven lives that when time spent on apps is compared time spent on the mobile web, apps are persistently the winner (Chaffey 2018).

Apps have unquestionably influenced our digital behavior, for better or for worse. Within the first few years of their existence, most users, including myself, were often unaware of or indifferent to the personal data and information certain apps collected that was then shared with device manufacturers, app vendors, and even third parties. It seems that the right to privacy in the world of apps, circa 2008–12, was an elusive and nebulous concept to most

smartphone users. In 2010, two journalists, Thurm and Kane from the *Wall Street Journal* claimed that many Android and iPhone apps breached the privacy of smartphone users (see article *Your Apps Are Watching You* 2010), since many apps have the capability to automatically capture a broad range of user information, including the user's precise location, phone number, list of contacts, call logs, unique device identifiers, and personal identifiable information. Thus, smartphones were the perfect tool to track personal user behavior and data. Paul Ohm, Professor of Law at the Georgetown University Law Center, calls them tracking devices and not phones (Maass and Rajagopalan 2012).

Smartphone technology continued to get more powerful with every year and the concept of privacy in the digital age was changing its meanings and its boundaries. According to Scoble & Israel (2014), "privacy is complex, fluid and granular. How much of it we want depends on many variables. Facebook used to let people respond to their relationship status, as 'It's complicated.' We think the same option can be used for privacy" (Scoble and Israel 2014, chap. 12). Not only are there multiple and often conflicting definitions of privacy in the digital age, but the issue also gets even more complicated when it is framed within the context of current laws regulating it. Europe proposed a reform of its data protection law in 2012, which has been in effect as the General Data Protection Regulation since May 25, 2018. While the United States does not have an all-encompassing data and privacy protection law, some governments and trade stakeholders argue "that the American approach — sector-specific privacy laws, in addition to industry self-regulation and enforcement by the Federal Trade Commission — is more nimble" (Singer 2013, para. 11). Even though it is not a law per se, the third resolution on "the right to privacy in the digital age" adopted by The United Nations General Assembly in December 2016 stated that

> the rapid pace of technological development enables individuals all over the world to use new information and communications technologies and at the same time enhances the capacity of governments, companies, and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy. (General Assembly 2016, 2/6)

The global public outcry that emerged in 2018 over the Facebook/Cambridge Analytica data privacy breach scandal proves that data/information privacy has finally become a global "hot" topic.

As they have with earlier technologies, libraries have worked to stay ahead of how its patrons (and the public in general) interact with smartphones and other mobile devices, and how that changes the role of the library in society. Numerous articles, books, and conferences, such as the first international m-libraries conference established in 2007 (but ceased after 2014), attest to this. The objective of the m-libraries conference was to "explore and share work carried out in libraries around the world to deliver services and resources to users 'on the move', via a growing plethora of mobile and hand-held devices" (dempsey 2008, para. 6). Utilizing mobile technology trends, libraries and librarians sought to "enter a new realm of importance to users" (Oberlies 2015, 3).

The same can be said about libraries and privacy, since librarians and information scientists have also been at the center of privacy and information technology debates.

For example, The International Federation of Library Associations and Institutions (IFLA) endorsed its Statement on Privacy in the Library Environment at its 2014 annual meeting. It stated that "data protection and privacy protection should be included as a part of the media and information literacy training for library and information service users. This should include training on tools to use to protect their privacy" ("IFLA Statement on Privacy in the Library Environment" 2015, para. 9). In the United States, The American Library Association (ALA) established its Privacy Toolkit (admin 2007) to educate librarians on how to protect patrons' privacy.

In 2010, the ALA's Choose Privacy Week (*Programs* n.d.) was launched to highlight privacy rights in the digital age for the library science profession. This initiative has been renamed and revamped as of June 2018, so that it " emphasizes the year-round importance of privacy and data security in today's libraries" (Stroshane 2018, para. 2).

Numerous other privacy initiatives related to libraries are currently underway or being developed in the United States, including the Library Freedom Project ("Library Freedom Project – Making Real the Promise of Intellectual Freedom in Libraries." n.d.), Data Privacy Project ("Data Privacy Project" n.d.), and the report "Library Values & Privacy in our National Digital Strategies: Field guides, Convenings, and Conversations" (Zimmer and Tijerina 2018).

Meanwhile, German librarians and libraries have also addressed the issue. The German Library Association[1] *(Deutscher Bibliotheksverband e.V. / dbv)* features links on data privacy law on its website, while the German Library Association *(Deutscher Bibliotheksverband / dbv)* hosted a panel discussion on the topic at the 2015 annual library conference (*DBT_2015_05_29_Datenschutz_in_Bibliotheken_endg. Pdf* - n.d.). More recently, the Association of German Librarians *(Verein Deutscher Bibliothekarinnen und Bibliothekare e.V.)* hosted a workshop about the new European Privacy law and its implication for libraries[2] .

1.2 Personal Background

As this dissertation is grounded in ethnography, the human is the (research) instrument (Fetterman 2010, 61). The "use of the first person in anthropological articles has always been fairly common" (Seadle 2000, 372) and thus I will use the first person in chapters where my voice, as the ethnographer, enriches this study. Moreover "the identification of the researcher's self within research texts acts to improve validity by demonstrating how data collection and data analysis may have been affected by the researcher's subjective reality" (Krenske 2002, 285). The chapters using the first person are the introduction, findings Fieldwork 1 and 2, discussion Fieldwork 1 and 2 and the conclusion.

There is no one definition of what ethnography is, since it is "used in diverse ways in a wide range of disciplines drawing on different traditions" (O'Reilly 2012, 1). I like Given's (2008) rather simple but straightforward definition:

> Ethnography is the art and science of describing a group or culture. The ethnographer enters the field with an open mind, not with an empty head […] The ethnographer is interested in understanding and describing a social and cultural scene from the emic or insider's perspective. The ethnographer is both storyteller and scientist; the closer the readers of an ethnography come to an understanding of the native's point of view, the better the story and the better the science. (2008, 288)

First, I will address my professional experience. I worked for over seven years as Web and Mobile Services Librarian/Assistant Professor at the Leonard Lief Library, Lehman College, part of The City University of New York. Teaching information literacy skills was one of my core responsibilities. I embraced the library's philosophy of inquiry-based learning, empowering

[1] All German texts, if not otherwise noted, have been translated to English by the author of this dissertation

[2] *VDB - Verein Deutscher Bibliothekarinnen und Bibliothekare: Datenschutz: Grundlagen. Umsetzung der EU-Datenschutzgrundverordnung in Deutschland* 2018

students' critical thinking skills. By 2011 I had developed, mobile information literacy sessions for Lehman College's Freshmen Year Initiative (Havelka 2013). As part of some of these sessions, students had to evaluate different apps by applying a modified Currency, Relevance, Authority, Accuracy Purpose (CRAAP) test[3]. Here are some questions:

Does the app have a privacy statement or setting? Does the app share information on social networks? Does it use location services?"

Initially, the students in this survey seemed unfazed or not concerned by privacy issues concerning apps, but then in the 2013–14 academic year, I perceived a small shift when it came to location sharing. Suddenly some of the students were more aware of privacy – they did not want app location tracking on their phones without prior consent and knowledge. At the same time, the app game Fruit Ninja, which was popular among the students at my university, received media attention in the US (for example, (*App Developers Are Tracking Kids despite Laws to Protect Their Privacy* 2014) and (Beres 2014)). This sparked my curiosity about apps and privacy research.

Besides teaching, developing a research agenda and then scholarly output was another integral part of my tenure-track librarian position. Early in my academic career, I focused on mobile learning, mobile information literacy, and mobile technologies in relation to academic libraries. Later, I also developed a research interest in libraries and privacy, and became Co-Chair of the Library Association of the City University of New York Privacy Roundtable[4]. Fostering privacy education among my peers and students was at the core of my privacy awareness agenda. Not only did I attend several Data Privacy Project workshops, but I also organized privacy training workshops for faculty, staff, and students at Lehman College. While attending these workshops, I noticed that most privacy training focused on desktop/laptop computers, but did not include any privacy training about mobile devices. This led me to an initial literature search for scholarly articles on the convergence of mobile technologies, apps, and privacy.

My own cultural experience played the second integral influence in my interest for the development of the research topic. As an immigrant from Germany to New York City in the

[3] see http://tiny.cc/lehmaninfoliteracy

[4] see https://lacuny.org/Privacy-Roundtable

United States, I was attuned to the cultural similarities and differences of the students and librarian peers at my faculty – not only as an outsider but also as an insider. With the emergence of social networks, mobile devices, and apps, I noticed through personal conversation with my friends and relatives back in Germany that their privacy attitude and behavior differed from that of my American friends, coworkers, and students. For example, many of my German friends perceived the rise of Facebook as a threat to personal privacy and thus chose not to have any Facebook presence at all. I began to wonder, was this due to Germany's stricter privacy law or because of Germany's cultural and historical past?

At the same time, I noticed that some of my American friends tended to overshare private details and information on social network sites. The combination of these two personal factors led me to develop my research question. The literature review (Chapter 3) will show that, to my current knowledge, no intercultural ethnographic study has researched mobile privacy, apps, and user behavior and attitude in the context of the library and information science students.

2. Research Question

This is the core research question:

> **Are there differences in the mobile privacy user behaviors and attitudes of American and German library and information science students?**

In order to establish the adequate context for the research, the following needs clarifications:

1. Mobile privacy entails personal data and information being accessed or transferred onto mobile devices to device manufacturers, app developers, and other third parties – and if or how it is controlled and or protected. It is not the purpose of this study to research privacy user behaviors and attitudes on desktop/ laptop computers, wearable devices (smartwatches, fitness trackers), and the Internet of Things (IoT). The reasons for limiting this study exclusively to smartphones are the following:
   First, tablet sales have steadily declined in recent years (*Player 3 Has Joined the Game – Chrome OS Detachable Tablets Paint a Brighter Future While Tablet Market Struggles, According to IDC* n.d.).

   Second, the focus lies on the research subjects' primary mobile device, which in most cases is a smartphone and not a tablet.

2. To define the term personal data, personal information, and personal identifiable information, GDPR Art. 4 (EU general data protection regulation 2016/679 in effect since 25 May 2018) is used:

   > "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (*Art. 4 GDPR – Definitions* n.d.)

3. At times the terms smartphone, cell phone, and mobile phones are used interchangeably in this dissertation. For this study a smartphone is a phone that has a touchscreen and can install apps via an app store. Further, a smartphone is much closer to a computer than what was previously considered a phone. The commercially successful era of the smartphone began with Apple's introduction of the first iPhone in 2007 and the release of

the App Store in 2008 ("iPhone App Store Downloads Top 10 Million in First Weekend" 2008).

4. The term "mobile privacy" occurs in the scholarly literature (see Biswas, Aad, and Perrucci 2013; Wang et al. 2016; Wijesekera et al. 2017) and will be the primary term used in this dissertation. However, at times the broader umbrella terms privacy and its digital subthemes are referenced, addressed, or discussed.
5. User behavior is defined as how a study participant utilizes smartphones, apps, and mobile websites in everyday life.
6. User attitude explores the feelings and established perceptions of study participants.
7. Some confusion between the terms privacy and security seems to exist (see, for example Bambauer 2013). Even though both are closely connected, mobile security is concerned primarily with, among other things, malware, viruses, spam, encryption, password protection, etc. on mobile devices. Although this research will address mobile security to some extent, it is beyond the scope of this dissertation to investigate security in-depth as it relates to mobile devices, mobile websites, and apps.

3. Literature Review

3.1 Overview

Privacy and its related subtopics have held the attention of scholars for quite some time. Nevertheless, this chapter will also demonstrate that qualitative research methods are still underrepresented. Other scholars and reviews have also validated this claim. **White and Grant** (2018) assert that:

> most of the studies on data privacy were quantitative, and there were very few qualitative studies which we could draw upon. Where possible, qualitative studies were included within the review. Given the general low level of understanding or conformity around many data privacy concepts or implications, there is a clear need and opportunity for more qualitative research to explore and interrogate why people think and behave the way they do. (2018, 24)

The next subchapter starts with defining privacy and then moves on to current research on the privacy paradox. Then German and American culture examined before moving into the issues of cultural research and privacy. Because ethnography is intertwined with culture, a pause on privacy is taken with a discussion of ethnography in general as well as in the library and information science discipline. The objective here is to set the stage for the discussion of the research method that follows.

The last two subchapters depict mobile security and mobile privacy research.

The summary emphasizes the justification for investigating mobile privacy from an ethnographic intercultural perspective.

3.2 Privacy Concepts and Definitions

What is privacy? If one asked a group of strangers on the street, it can be assumed that they would not only be a bit startled and have some difficulty coming up with an answer, but that their definitions would differ. **Benjamin** (2017) supports this notion:

> Privacy has become a convoluted, murky, and often contradictory term in the information age. The complexities and counterarguments to any position on privacy in contemporary society hark back to a divided history of the term and herald the potential for even greater confusion and exploitation in the future. (2017, 55)

Privacy and its related terms (information privacy, online privacy, and data privacy) as well as surrounding topics have been and will continue to be discussed and researched by a myriad

of different scholars in such different disciplines as law, ethics, computer and information science, psychology, education, and library science. To put mobile privacy in context, the various definitions of privacy and information privacy are briefly discussed; some of the older privacy definitions are certainly still relevant in the mobile device era.

In his famous book *Privacy and freedom*, **Westin** (1967) connected privacy with control and self-determination. In his definition:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. (1967, 7)

Ware was among the first scholars to first intertwine privacy and computer technology. In 1977 he presented a paper on Computers and Personal Privacy (Ware 1977) at the Symposium on the Computer and American Society. As he wrote, "Privacy is used in an information context. It does not allude to intrusion into one's physical, psychological, or physiological space.

Formally, it can be defined as follows per Ware (1977, 356):

> It is the social expectation that the individual
> 1. will have some say in how information about him is used, to whom it is communicated, and how it influences him.
> 2. will have some protection against unwarranted harm because of the functioning of some record-keeping system and will be treated fairly by such systems.
> 3. has protection against unwelcome, unfair, or intrusive collection of information". (1977, 356)

In the mid-1990s, with the Internet still in its infant age, the legal scholar **Anita Allen** (1998) looked at privacy from three different angles – physical, proprietary, and informational privacy. She defined informational privacy as "confidentiality, secrecy, data protection, and control over personal information"(1998, 723). The author also mentions how the erosion of privacy might happen due to technological advancements (cellphone, fax, email) and how these advancements might make it easy for the government and the private sector to collect information about each individual. She noted, "Technologists hope that someday soon we may be wearing computers capable of transmitting data around the world"(1998, 735).

More recently, two information systems researchers, **Bélanger and Crossler** (2011) wrote an in-depth review article on the state of information privacy in information system research. The authors admitted that:

> There are many definitions for information privacy, but there is little variance in the elements of the definitions, which typically include some form of control over the potential secondary uses of one's personal information (Bélanger et al.2002). Secondary use refers to the practice of using data for purposes other than those for which they were originally collected. (2011, 1081)

In their conclusion, they suggest several future research directions:

- taking into account different nations' or cultures' perceptions of information privacy and its surrounding issues (2011, 1026–27);
- using ethnography, case studies, and action research to study information privacy issues at the organizational level (2011, 1035);
- moving away from relying solely on US participants as research subjects (2011, 1035);
- comparative analysis of non-students with students as well as international participants with US participants (2011, 1035).

3.3 Privacy Paradox

In the research literature, the discrepancy between privacy behavior and attitude is called the privacy paradox. Because this research investigates privacy behavior and attitude in a mobile and cross-cultural setting, the privacy paradox is briefly examined.

Among the first to use the term "privacy paradox" was **Barnes**, in 2006. Barnes framed in her article the privacy paradox as behavior and attitude conducted mostly by teenagers and students on social networking sites (Friendster, Myspace, Facebook). She noted, "Marketers, school officials, government agencies, and online predators can collect data about young people through online teenage diaries. Herein lies the privacy paradox. Adults are concerned about invasion of privacy, while teens freely give up personal information" (2006, para. 20). She brought up the example of a survey in which teenagers were asked about how they would feel if their personal statements on social networking sites were made public. Most of the responses were neutral in terms of attitude, yet in terms of behavior, the students acted as if social networking sites were private and not available to the public. Concluding, she remarks, "the root of the privacy paradox is the collection and control of personal information …

Moreover, social networking companies and advertisers need to establish policies about the proper use of personal information posted on these sites" (2006, para. 46).

Two more recent articles review research and literature on the privacy paradox (Kokolakis 2017, Barth and de Jong 2017).

Kokolakis (2017) affirms that the "dichotomy of information privacy attitude and actual behaviour has been coined the term "privacy paradox" (Brown, 2001; Norberg et al., 2007) or, to be more accurate, "information privacy paradox"(2017, 123). While there has been much research about it in the last 20 years, Kokolakis' article's objective is to survey scholarly literature to find out whether the information privacy paradox exists and, if so, how it can be explained. It must be noted that Kokolakis focuses on information privacy and excludes scholarly articles investigating the privacy paradox from a legal or ethical perspective. Starting with early studies such as Sayre and Horne (2000), Spiekermann, Grossklags, and Berendt (2001), and Acquisti (2004), the author then highlights studies supporting the privacy paradox.

Among them is a more recent one by Taddicken (2014). Taddicken used an online survey and found out that "privacy concerns hardly impact self-disclosure" (2014b, 125). Counterbalancing these studies, Kokolakis turns his attention to research questioning the existence of the privacy paradox, such as by D'Souza and Phelps (2009), Lutz and Strathoff (2014), Young and Quan-Haase (2013).

In the last paragraph of his essay, Kokolakis gives an excellent overview of different interpretations of the privacy paradox based on five different research areas: privacy calculus theory (see also below), social theory, cognitive biases and heuristics in decision-making, decision-making under bounded rationality and information asymmetry conditions, and quantum theory homomorphism. Concluding his literature review on the privacy paradox, the author gives several recommendations, such as "future research could also focus on specific age and cultural groups, such as elderly individuals, rural cultural groups, etc." (2017, 132).

The systematic literature review of the privacy paradox undertaken by **Barth and de Jong** (2017) differs from those above inasmuch as the authors' aim is to "attempts to develop an overarching theoretical framework, addressing the discrepancy between privacy concerns and actual online protective behavior through different theoretical lenses with a special focus

on mobile applications" (2017, 1040). Since the authors could only identify nine studies investigating the privacy paradox and mobile application, they broadened their literature review to the online realm as well. In their discussion, the authors highlight some specific findings on mobile applications and privacy paradox and caution that "comparing the results from social network studies with those focusing on mobile application usage, it seems that the privacy paradox within the mobile context is even more complex" (2017, 1051). Barth and de Jong posit a few possible solutions on how to break through the privacy paradox, such as privacy awareness or including privacy prompts in apps. Concluding, they argue that "future research on the privacy paradox should try to measure actual behavior in order to get better insights into the problem" (2017, 1052).

3.4 German and American Culture

Before reviewing any of the literature that juxtaposes cultures and privacy in general as well as interculturally between Germany and America, an outline and comparison of both nations is given below. Furthermore, a short overview of the history and laws concerning privacy and data protection in both countries is provided.

3.4.1 Hofstede's Cultural Dimension: Germany versus the US

Several of the multinational studies, as well as Germany versus US literature, use **Gert Hofstede's** cultural dimension model to compare different cultures (see below). In earlier work, Hofstede defined five cultural dimensions: see (Hofstede, Hofstede, and Minkov 1991; Hofstede 2001).

Here the six dimensions described in Hofstede's more recent work (Hofstede 2011) to compare Germany and the US will be used. They are:

1. Power Distance: "the extent to which the less powerful members of organizations and institutions (like the family) accept and expect that power is distributed unequally" (Hofstede 2011, 9).
2. Uncertainty Avoidance: "deals with a society's tolerance for ambiguity. It indicates to what extent a culture programs its members to feel either uncomfortable or comfortable in unstructured situations" (Hofstede 2011, 10).

3. Individualism versus Collectivism: "cultures in which the ties between individuals are loose: everyone is expected to look after him/herself and his/her immediate family. On the collectivist side, we find cultures in which people from birth onwards are integrated into strong, cohesive in-groups, often extended families" (Hofstede 2011, 11).

4. Masculinity versus Femininity: "refers to the distribution of values between the genders" (Hofstede 2011, 12).

5. Long Term versus Short Term Orientation: "every society has to maintain some links with its own past while dealing with the challenges of the present and future" (*Country Comparison Germany and USA* 2019).

6. Indulgence versus Restraint: "Indulgence stands for a society that allows relatively free gratification of basic and natural human desires related to enjoying life and having fun. Restraint stands for a society that controls gratification of needs and regulates it by means of strict social norms" (Hofstede 2011, 15).

The following graphic compares these six dimensions in Germany and the United States:

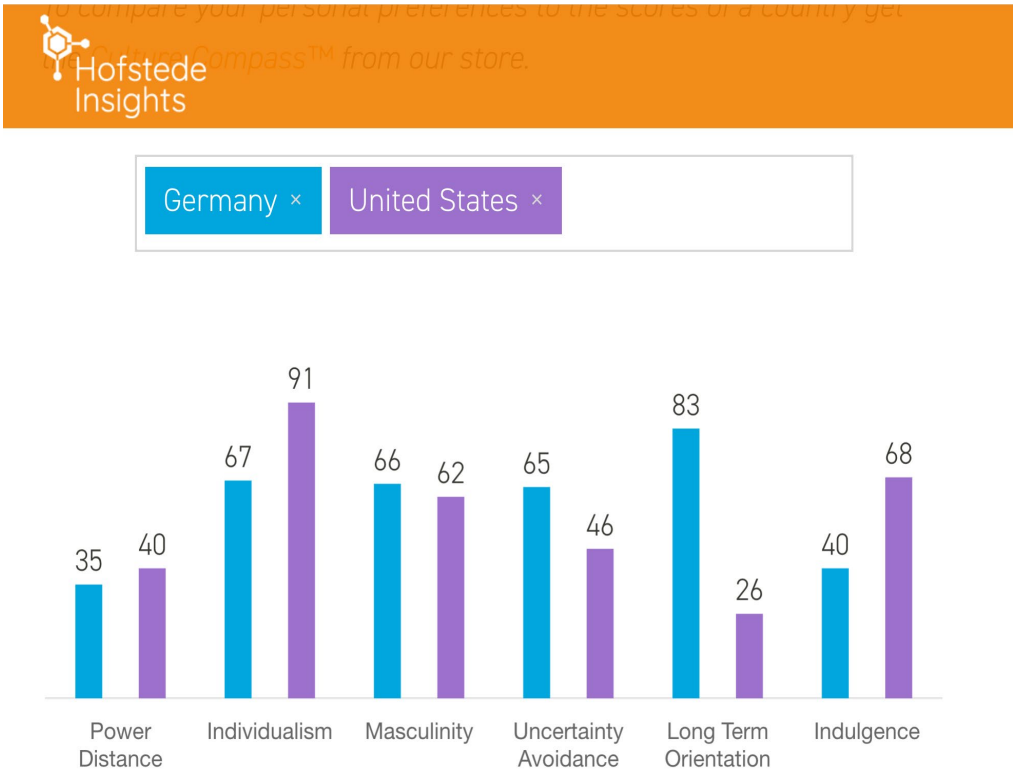

Figure 1 Six cultural dimensions to compare Germany and the US;
Accessed on January 20, 2020.
https://www.hofstede-insights.com/country-comparison/germany,the-usa/

Some of the dimensions, such as Power Distance and Masculinity, had relatively close scores in both countries. The dimensions with more divergent scores warrant further explanation which are Individualism, Uncertainty Avoidance, Long Term Orientation, Indulgence.

Individualism: Germany scores lower on the individualism dimension. While both are individualistic countries, in the United States "society is loosely-knit in which the expectation is that people look after themselves and their immediate families only and should not rely (too much) on authorities for support" (*Country Comparison Germany and USA* 2019, para. 2). In Germany, "There is a strong belief in the idea of self-actualization. Loyalty is based on personal preferences for people as well as a sense of duty and responsibility" (*Country Comparison Germany and USA* 2019, para. 2).

Uncertainty Avoidance: Countries with a higher score prefer clarity and structure are more prone to emotional stress and anxiety, and are less tolerant of different ideas or behavior. For example, Germans have a reputation for being punctual, organized, and orderly. The German word *Angst* (a subtler version of fear) does not need an English translation, as it is understood and used in the English language too.
Americans are perceived as open to new ideas, innovative when it comes to technological development, and ready to embrace unforeseen challenges.

Long Term Orientation: On this dimension, Germany and the United States have a 57-point difference.

> Germany's high score of 83 indicates that it is a pragmatic country. In societies with a pragmatic orientation, people believe that truth depends very much on situation, context, and time. They show an ability to adapt traditions easily to changed conditions, a strong propensity to save and invest, thriftiness, and perseverance in achieving results. (*Country Comparison Germany and USA* 2019, para. 13)

Those living in the US, on the other hand "are prone to analyse new information to check whether it is true. Thus, the culture does not make most Americans pragmatic, but this should not be confused with the fact that Americans are very practical, being reflected by the 'can-do' mentality mentioned above" (*Country Comparison Germany and USA* 2019).

Indulgence: The United States scores higher on this dimension. In the US, people like to flash their wealth and success more. They like to treat themselves, for example, to the newest and latest gadgets. Overall, Germans are less optimistic and joyful and tend to be more restrained.

3.4.2 Privacy and Data Protection History

Germany's history in the 20th century differs quite dramatically from the United States'. Two main periods have influenced the Germans' perceptions and attitudes about privacy and data protection.

1. The first is the Nazi time (during German Reich until 1945) during which personal data collection was abused to identify Jews and other minorities systematically (Freude and Freude 2016, 2).
2. The second one was (during the GDR regime 1949–1990), when East Germany's State Security Service (*Staatssicherheitsdienst)*, known as the *"Stasi"*, engaged in mass surveillance of its citizens (1950–1989) and or neighbors, coworkers and friends spying on each other.

As a result of these dark historical times, "Germans place a great deal of importance on privacy and data protection. Fear of the private sector and, even more so, government abuse of personal data is widespread" (Freude and Freude 2016, 1). A study investigating the attitudes of consumers from five different countries (US, China, UK, Germany, and India) toward data protection revealed that "Germans, for instance, place the most value on their data, and Chinese and Indians the least, with British and American respondents falling in the middle" (Morey, Forbath, and Schoop 2015, 100). Going back to Hofstede's cultural dimension, people from more individualistic countries such as Germany and the US may value personal information more than people from more collectivistic countries such as India and China (Morey, Forbath, and Schoop 2015, 100).

Privacy in the US has not been influenced by dramatic historical events to the same extent as it has in Germany. Yet according to **Palmer** (2011) there are three landmark changes in how privacy has been perceived in the US. These are:

1. Warren and Brandeis's famous 1890 article on privacy. In it the "authors wisely made no attempt to claim that privacy was an ancient 'natural right' or a liberty interest protected under the constitution. Nor did they boldly seek to be the first to delimit the meaning of privacy. As we know, they only borrowed memorable phrase of Judge Cooley that it was the right 'to be let alone' "[5] (2011,73).
2. Prosser's 1960 article on privacy, in which he stated that "the right of privacy had been recognized by the overwhelming majority of the American courts and would probably soon be recognized by more. As of 1960 it had been rejected in only three or four states. Yet, he cautioned, only lately has there been any attempt to inquire what interests are we protecting, and against what conduct" (2011, 83).
3. And then also in the mid 60s there was further change: privacy was no longer seen as a liberty. Instead, it was a constitutional right. Now the "right of privacy was a nationwide guarantee" (2011, 94).

3.4.3 Privacy and Data Protection Laws

Not only do the US and Germany diverge historically in their views about privacy and data protection, but their law or laws have also been and are quite different. According to **Ybarra**, "Germany has some of the strictest data collection laws in the world" (2011, 293).

Krasnova and Veltri (2010) also link this back to Hofstede's cultural dimension:

> Hofstede [10] argues that to deal with uncertainty societies high on UAI [Uncertainty Avoidance] adopt strict rules, laws, and policies to minimize uncertainty. This is also true for the privacy-related legislation. For example, whereas privacy protection in the USA – [a] country low on UAI – is, in most cases, left to industry self regulation, Germany has a large body of laws aiming to protect privacy of its citizens [4]. (2010, 3)

In Germany, the first data privacy law was established in the federal state of Hessen in 1970 (Calderón 2017, 23). Other federal states followed with data protection acts, and then in 1978, the Federal Data Protection Act *(Bundesdatenschutzgesetz)* became the official law. Over the years, this law went through several revisions, most recently in 2017. Of particular relevance for Internet and information technology data was the creation of the Tele Media Act in 2007,

[5] Warren & Brandeis, supra note 10, at 194.

which "stipulated the duty to safeguard data protection during the operation of telemedia services" (Stepanova, 2018, 146).

Since Germany is a member of the European Union, two other European laws govern data privacy there. The first is the General Data Protection Regulation (E.U.) 2016/679 (GDPR[6]), whose predecessor was the European Data Protection Directive of 1995.

The GDPR became law in May 2018. As a European law, the GDPR trumps the German Federal Data Protection Act as well as the Tele Media Act.

The new law has many facets, such as privacy by design[7], the right to be forgotten, and the right to be informed.

> There is a need for transparency regarding the gathering and use of data in order to allow E.U. citizens to exercise their right to the protection of personal data. Therefore, the General Data Protection Regulation (GDPR) gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller. The law differentiates between two cases: On the one hand, if personal data is directly obtained from the data subject (Art. 13 of the GDPR) and, on the other hand, if this is not the case. (Art. 14 of the GDPR). ("Right to Be Informed" n.d., para. 1)

The second European law is the ePrivacy Directive of 2002, which is currently under revision and may soon become the ePrivacy Regulation[8]. The ePrivacy Directive aims to "sets out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also bans unsolicited communications where the user has not given their consent."(*Directive 2002/58/EC of the European Parliament and of the C... - EUR-Lex* n.d., para. 14)

In the United States, data privacy is managed quite differently. First of all, no all-encompassing federal data privacy law currently exists. Though the United States introduced a Privacy Act in 1974, which "provided a broad set of information privacy protection, it only applied to federal agencies, not the private sector" (Newman and Tijerina 2017, 27).

[6] In this study GDPR stands for General Data Protection Regulation.

[7] https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html

[8] In October 2019 the Council of EU Member States released a new draft version of the ePrivacy Regulation ("EPR"): https://www.insideprivacy.com/international/european-union/new-draft-eprivacy-regulation-released/

In 2010 the United States came close to establishing a consumer data privacy law when a bill to strengthen online privacy rights was proposed.

> [This] proposed bill expanded the definition of sensitive information to include an individual's Internet Protocol (I.P.) address, name, race or ethnicity, precise location, or any user-entered preference profile. Hence, if any of this personal information could be used to identify a user, companies would be required to provide users with notice. The proposal would require companies to include descriptions of how the information is collected, stored, and the duration of the data storage. (Ybarra 2011, 276)

However, in the end, the bill did not pass, and to this day, the United States data privacy protections remain a mix of industry self-regulation and a patchwork system of different sector-specific federal law as well as state laws. These federal laws include, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Children's Online Privacy Protection Rule ("COPPA").

> COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. ("Children's Online Privacy Protection Rule ('COPPA')" 2013, para. 5)

With the implementation of the GDPR, more and more voices have emerged to argue that the US needs to have its own national privacy law. As the Economist puts it, "America rarely looks to the bureaucrats of Brussels for guidance. Commercial freedom appeals more than *dirigisme*. But when it comes to data privacy, the case for copying the best bits of the European Union's approach is compelling" (*The Economist* 2018, para. 1).

In the meantime, some states such as California, Nevada, and Maine have passed laws to protect consumers' online privacy levels at the state level, with many others proposing or discussing bills (*U.S. State Comprehensive Privacy Law Comparison* n.d.). California's Consumer Privacy Act is set to become the law in January 2020 and is supposed to "have de facto application to businesses operating across the United States" (Raul and Mohan, 2018, 384).

3.5 Privacy and Cultural Research

Different scholars have investigated privacy issues by examining different cultures' attitudes and behavior. I will first review the literature with a multinational focus. The final part of this

subchapter reviews the literature specifically comparing privacy issues between Germany and the United States.

3.5.1 Multinational Research

One older article worth mentioning is **Altman's** *Privacy regulation: Culturally universal or culturally specific?* (1977). Even though this article was published before mobile technologies or the internet became an everyday global realities, it brings up valuable viewpoints on culture and privacy. Altman posits that although the "capability for privacy regulation may be culturally universal, the specific behaviors and techniques used to control interaction may be quite different from culture to culture" (1977, 69). He strengthens his claim by pointing to ethnographic evidence of privacy behavior among different cultures. Here Altman mentions several cultures with minimal privacy – among them, for example, the Mehinacu Indians from Brazil or the Javanese. He next counterbalances these with cultures that seem to have maximum privacy behavior, such as the Balinese or Tuareg. He points out then that "once again, these examples illustrate how privacy is a culturally pervasive process if one views it as the presence of forces for people to make themselves more or less accessible to others" (1977, 77). Concluding, Altman admits that his article takes a unique approach since it considers privacy behavior as a social and psychological process closely intertwined within unique cultural norms and settings.

Some more recent articles research online privacy and culture in a multinational context are by **Bellman et al.** (2004), **Hichang Cho, Rivera-Sánchez, and Sun Sun Lim** (2009), **Sheth, Kaiser, and Maalej** (2014) and **Omrani and Soulié** (2017). All of them, with the exception of **Sheth, Kaiser, and Maalej** (2014), apply Hofstede's dimension model to look at cultural values. However, one commonality is that all researchers used a quantitative research methodology in the form of online surveys. Only Sheth, Kaiser, and Maalej (2014) collected small qualitative findings by including two open-ended questions in their survey. The overall consensus of all these researchers is that culture differences matter for privacy concerns, behavior, and attitude. For example, Cho, Rivera-Sánchez, and Sun Sun Lim (2009) propose that "rather than assuming that the online population is homogenized due to the forces of globalization, governments and corporations must be cognisant of the prevailing cultural and individual

differences that influence internet users' behaviour vis-à-vis online privacy" (2009, 411). With Sheth, Kaiser, and Maalej (2014) stating:

> Our analysis for geographic regions, for example, shows that there is a significant difference between respondents from North America, Europe, and Asia/Pacific. People from Europe and Asia/Pacific rate different types of data such as metadata, content, and interaction data being a lot more critical for privacy than respondents from North America. People from Europe are a lot more concerned about data breaches than data sharing, whereas people from North America are equally concerned about the two. (Sheth, Kaiser, and Maalej 2014, 860)

Although Bellman et al. (2004) perceive culture as an influence on online privacy concerns, they are also a bit more cautious, stating that " in our sample, the influence of cultural values was only seen in two dimensions of information privacy concerns, errors in databases and unauthorized secondary use, rather than in overall concern for information privacy (CFIP)" (2004, 8).

In 2011 **Trepte and Masur** (2016) analyzed in a multicultural online survey study social media use, culture differences, and privacy attitude behavior of five different nations (the United States, the United Kingdom, Germany, the Netherlands, and China). Although this study's research method is quantitative, some findings are applicable toward this research:

- People from all countries indicated having high privacy literacy. Participants from Germany and the US perceived themselves as slightly more literate than participants from other countries.
- Europeans and in particular Germans reported perceiving information as more sensitive and reported believing that privacy-related behaviors such as posting one's relationship status affect their privacy.
- US American and Chinese social media users generally posted more sensitive information online than Europeans (Trepte and Masur 2016, 5).

The most crucial part of this in-depth study was the assessment at the end. On one hand, the authors acknowledged that there seems to be more cohesion than difference between different cultures regarding privacy. Here the authors assume this might be due to digital globalization. Nonetheless, the authors "believe that culture has a significant influence on the perception, evaluation, and handling of privacy. Looking at cultural dynamics and understanding how new media transform our traditional beliefs about privacy thus seems to be of utmost importance." (2016, 71)

In 2014 **Miltgen and Peyrat-Guillard** published their article *Cultural and generational influences on privacy concerns: a qualitative study in seven European countries*. They used focus groups in Romania, Greece, France, Estonia, Spain, Poland, and Germany.

Of particular interest were some of the qualitative findings, such as opinions on personal data management in different European countries: "One has not really got a choice. For example, when pursuing some goal such as getting a new email address or a new account. One is basically forced to do it (German participant)" (2014, 15). Furthermore, "it depends on the data you disclose; it depends on how close to me they are and on how private and secure this data is (Greek participant)" (2014, 14–15). Furthermore, on privacy and control, "but I believe that we're going more and more toward the breach of privacy of people, and we're going more and more toward dictatorship (French participant)" (2014, 16). Or on protection and regulation: "That's the problem, they're always legally covered. Lawyers aren't stupid. That's why they write these endless pages because they want to insure themselves against everything. But if protection were greater, we probably wouldn't be sitting there (German participant)" (2014, 17).

One common result for the European countries covered is the concern about data disclosure (2014, 19). And another exciting finding associated with culture is that:

> some key cultural and generational differences appear, including a north–south divide regarding the significance of responsibility versus trust. Issues of control and choice also prompt different perceptions: In the south, people believe they have a choice, whereas, in Eastern Europe, people believe they are forced to disclose … (2014, 30)

In the conclusion the authors, Miltgen and Peyrat-Guillard point out that their study is one of the few qualitative studies to directly quote the privacy opinions and attitudes of European citizens.

3.5.2 Intercultural: Germany and America

Three articles by the same authors, **Krasnova and Veltr** (2010, 2011), are all based on the same quantitative research methodology and data compared German and American culture, social networking site self-disclosure, and the privacy calculus, which is how users weigh the perceived risk and benefits of disclosing information (Krasnova and Veltri 2010, 2011; Krasnova, Veltri, and Günther 2012). Similar to other researchers, the authors used Hofstede's cultural dimensions to compare Germany and the United States. Some interesting findings:

> Users with high privacy concerns are expected to be more conscious about the information they share (…) Americans had higher concerns than Germans. This can be explained by higher levels of IDV [Individualism] and MAS [Masculinity] of American users (…) 22.8% of Americans claimed to be 'very much concerned 'about the fact that their information could be used in a way they did not foresee (Q1). This is twice the share of Germans (10.2%). Furthermore, high level of UAI [Uncertainty Avoidance] in a society typically leads to stricter laws which protect individuals. Empirical evidence shows that these laws may work to reduce privacy concerns of consumers [14]. This may explain the lower concerns of German SNS users as they rely on strong privacy regulation and hence are less concerned about information misuse. (Krasnova and Veltri 2010, 5)

In summary the authors found some evidence that German and Americans have different attitudes about privacy in social networking sites. As such the authors recommend social network site companies take their findings about awareness, trust building, and control into consideration in order to protect their customers' personal data and privacy.

3.6 Ethnography and Culture

Simply put:

> Culture is the broadest ethnographic concept. The classic materialist interpretation of culture is the sum of a social group's observable patterns of behavior, customs, and way of life. According to the cognitive approach, culture includes the ideas, beliefs, and knowledge that characterize a particular group of people. Ethnographers need to know about both cultural behavior and cultural knowledge to describe a culture or subculture adequately. (Given 2008, 288)

Ethnography is part of the field of anthropology, specifically cultural anthropology. Doing fieldwork, which is going into the field and becoming very similar to a native, always for a prolonged time while observing one particular social group or culture, was and is its most characteristic/distinctive feature. These days ethnography is widely adopted as a research method by many other disciplines, such as sociology, education, psychology, communication, computer science, and of course, library and information science.

3.7 Ethnography in Library and Information Science Research

It is beyond the scope of this subchapter to recap in-depth ethnographic research and practice in library and information sciences, as others already have done an excellent job (see Sandstrom and Sandstrom 1995; Goodman 2011; Khoo, Rozaklis, and Hall 2012; Ramsden 2016).

Furthermore, "the use of ethnographic methods to investigate bibliographic trends, library services, and information systems is not new. What is new is the increased publicity and attention that some library research projects have attracted" (Goodman 2011, 3).

Three library and information studies have distinguished themselves in this area, all of them for the same reasons. First, they all involved a professionally trained anthropologist/ethnographer. Second, they were all longitudinal studies, and third, responding to Sandstrom and Sandstrom's criticism on LIS and ethnography, they "embrace a broadly conceived research program resting on a foundation of scientific, anthropological methods" (1995, 192).

The first one, the University of Rochester's "Studying Students" Project (**Foster and Gibbons** 2007), applied ethnographic methods such as faculty and student interviews, surveys, and

mapping diaries to investigate how undergraduate students used an academic library and its various components (library website, space, librarians). This study garnered accolades and became prominent in depicting how ethnography as a research method supports librarians and libraries in creating a truly student-centered library.

The second one is the ERIAL project, (**A. D. Asher, Miller, and Green** 2012; *ERIAL Project* 2020), influenced by Foster and Gibbons' earlier work. It was a two-year study conducted in collaboration among five academic libraries in Illinois. Not only were the findings applied to make effective changes at all participating institutions, but Asher and Miller (2011) also created as practical toolkit helpful to any novice library ethnographer.

The third study was done by two librarians at my previous institution, the City University of New York. The CUNY Undergraduate Scholarly Habits Ethnography Project (*About This Study | Undergraduate Scholarly Habits Ethnography Project* n.d.; **Regalado and Smale** 2015) used "qualitative methods to examine the scholarly habits and explore the diversity of the undergraduate experience in the urban, public, commuter colleges that make up the CUNY system" (*About This Study | Undergraduate Scholarly Habits Ethnography Project* n.d.). Their chapter on *College Students and Mobile Technology* is highly relevant to my research, as within mobile devices, "smartphone usage predominated overall, with the majority reporting that they used their smartphones for academic work at least sometimes at home, on campus, and on the commute (Table 3.2)" (Smale and Regalado 2017, 44).

3.8 Mobile Security

As stated in the research question, mobile security is not the focus of this dissertation. However, as mobile security emerged as an issue in the findings, it's important to briefly discuss what mobile security is and how it differs from mobile privacy.

Jain and Shanbhag (2012) give a succinct overview of security issues in the mobile environment. These can range from physical device loss and theft to vulnerable application, malware, compromised devices, data interception, and mobile web browser exploitation. The authors then explain in greater detail the most prominent technical security risks for apps. Among them are weak server-side control, which controls security patches and updates; client-side interferences via "attacks such as abusing the phone dialer, SMS, and in-app payments" (2012, 31); and insecure data storage. To help information security professionals and app developers, the authors also give practical advice on how to release secure apps in the first place. While the article's focus is on mobile security, the authors briefly touch upon mobile privacy, as mobile security threats can "lead to the exposure of sensitive information, privacy violations, and noncompliance" (2012, 31).

Li and Clark (2013) argue that "security solutions [...] must defend against viruses, malware, botnets, intrusion attacks, threats amassed through the deployment of a wide spectrum of mobile applications, and attacks that are specific to mobile devices" (2013, 78). They point out that most smartphones user have a gap in both their knowledge and skills on how to be proactive mobile secure users. As their article's audience is the IT enterprise industry, they suggest an "infrastructure-centric security ecosystem with cloud defense" to foresee mobile security threats. Concluding, the authors point out how the protection of mobile devices is tantamount to the protection of one's privacy.

In the foreword to their book on *Mobile Security and Privacy: Advances, Challenges, and Future Research Directions*, **Au and Choo** (2017) provide a clear and focused overview of mobile security risks, dividing them into application-level, web-level, network level, and physical level threats. In the second chapter from the same book, Tully and Mohanraj (2017) explain these different threats in detail. They also describe mobile security technical controls, which include encryption, remote track, and wipe antivirus/antimalware and user training. Tully and Mohanraj claim, "user training is even more important than technical controls. An

educated user on a device with poor security is safer than an uneducated user on a device with 'strong' security"(2017, 40). Interlinking privacy to mobile security, the authors indicate how the need for privacy remains relevant and what the loss of privacy can mean for individuals and organization. Additionally, the authors give practical guidelines on what individuals should do to protect their privacy in the digital realm.

In conclusion, all of the articles mentioned above have the same foci in regard to mobile security, thus highlighting a similar understanding for the mobile security research community. Even though they all recognize a close relationship to mobile privacy, they also perceive mobile security as a distinct and separate research topic.

3.9 Mobile Privacy

Even though research on privacy as it relates to smartphones had been conducted before 2007, this review on mobile privacy starts from that year for two reasons:
First, although earlier smartphones such as the Blackberry Curve or the Nokia had email, web, navigation, and or camera features; the release of the first iPhone in 2007 was a game changer for the mobile industry, as was the Apple app store a year later. It was only then that smartphones become actual personal information and data tracking devices, and privacy in the mobile realm became a topic of greater interest to scholars. Second, older articles on mobile privacy tend to be technically outdated.
In the section below research on the topic is addressed in reverse chronological order.

One of the newest research studies of **Henke, Joeckel, and Dogruel** (2018) investigates the privacy behavior and attitude of German university students concerning smartphones. The authors postulate:

> Even though attitudes and concerns about privacy and their impact on behaviour have been extensively studied for Internet and Networking Site users (Dienlin and Trepte 2015; de Wolf et al. 2016), there is a lack of a deeper understanding of how attitudes and concerns influence the privacy behaviour of smartphone users. (2018, 489)

Defining privacy, they review prominent privacy scholars such as Altman (1975) as well as Dielin's (2014) newer Privacy Process Model. However, they note:

> With respect to mobile privacy, smartphone users' privacy is, to a considerable extent, not only a consequence of their self-disclosure behaviour but also determined by the apps they use and how they use these apps. For instance, users may give away personal information by turning on their phone's GPS function, or using an app that offers location-based services. (2018, 489)

Placing attitude-behavior into a theoretical framework, Henke, Joeckel, and Dogruel (2018) next mention several attitude-behavior scholars and their work. Interestingly they reported that some researchers found a relationship between these two, while others could not establish an influential link (2018, 489). According to the authors privacy attitude and behavior is composed of "elaborate, calculative information processing (Dienlin and Trepte 2015), but also of more spontaneous processes, such as heuristics (Acquisti, Brandimarte, and Loewenstein 2015; Dogruel, Joeckel, and Bowman 2015)" (2018, 490).

As their research method, Henke, Joeckel, and Dogruel adopted Fazio's Mode model, which in simplest terms names "motivation and opportunity as determinants of the attitude-behavior relationship" (Olson 2007, 584) toward the process of downloading apps. Unlike this study, which uses ethnography as its qualitative method, Henke, Joeckel, and Dogruel used a quantitative research approach in the form of five time-staged online surveys. In their findings, the authors confirm that activation of participants' privacy attitudes influences an app's permission setting and download process. However, they also caution, "Only under specific circumstances, such as automated attitude activation in spontaneous processes and behavioural intentions in elaborate ones, will privacy attitudes become predictors of concrete privacy-related behaviour" (Henke, Joeckel, and Dogruel 2018, 499).

Even though the objective of this dissertation is quite different both in its research method and overall objective (see chapter 4 and chapter 5), the article is relevant as it furthers understanding of behavior and attitude theories and research. Concluding, it would be interesting to expand the study and add a cultural component into it, either with a cultural background that is quite similar, e.g., from within Europe or with participants from a different cultural setting (e.g., Asia).

Some of the same researchers, were involved in the research study *The reliance on recognition and majority vote heuristics over privacy concerns when selecting smartphone apps among German and US consumers* (**Joeckel, Dogruel, and Bowman**, 2017). The topic is not based on behavior and attitude but on how and why consumers choose to download apps and whether privacy concerns play any part in the process (2017, 622). This article is of relevance since participants of this research also had to download an app (see chapter 4 Interview Schedule Fieldwork 1). The authors "also consider potential cultural variance in these app selection processes, given the social construction of brands and observed variance in cultural norms regarding information privacy" (2017, 625). According to the authors, other researchers such as Cho, Rivera-Sanchez, & Lim (2009), Salmona, Melton, & Miller (2013) have investigated how cultural differences matter when it comes to privacy concerns. Here the authors highlight two recent scholars who claim that Germans are more privacy-conscious than Americans (see Singh and Hill 2003; Bellman et al. 2004). They used a mixed research method using a quantitative observational study in combination with a qualitative retrospective think-aloud

protocol (2017, 626). Similar to this study, a relatively small number, 43 students, participated in the study, both chosen via convenience sampling from a US and a German university**.** Joeckel, Dogruel, and Bowman interspersed a few direct quotes from study participants into their results, which aligns with the objective of this study: to put a rich description at the heart of the results and discussion. It would have been advisable to include more verbatim quotes to the article, since they are rarely included in the current research literature on mobile privacy. Concluding the authors "acknowledge that different levels of privacy awareness on a cross-cultural level seem to be important determinations to even cursory concerns over data privacy. Future research is advised to account for these cross-cultural differences" (2017, 633).
This research does precisely this. Moreover, it will try to validate or refute whether cultural differences matter in relation to mobile privacy attitude and behavior.

Another cross-culture study from **Pentina et al.** 2016 explored the privacy paradox in information-sensitive mobile app adoption of American and Chinese students. The authors applied the privacy calculus theory and said this is "an attempt to explain the inconsistency between expressed privacy concerns and actual sensitive-technology adoption behavior, the privacy calculus theory suggests that in the process of decision making, consumers make mental tradeoffs between perceived benefits and perceived privacy risks" (2016, 409–10). In terms of culture, the authors looked at previous research such as Straub, Keil, and Brenner (1997); Meso, Musa, and Mbarika (2005); and Cao and Everard (2008). One common denominator of those studies was that culture is both an influence as well as a differentiator for technology perception and behavior. Pentina et.al used a quantitative approach via an online survey for both cultures; from this research method, the findings and particularly discussion of this article are valuable and relatable to this research (see chapters Finding Fieldwork 1 / Discussion Fieldwork 1). The authors admit that further research on investigating possible cultural variables and personal traits as one factor in new technology adoption should be conducted.

Lee and Song (2015) do not look at mobile privacy as such, but their research is one of the few comparing mobile habits across two distinctive cultures. The authors juxtaposed the mobile-information-seeking behavior of college students from the US and from South Korea.

Particularly of interest for this research are the findings on smartphone brand and mobile operating systems in use as well as students' favorite phone activities. "Almost 90% of KU [South Korea] students owned Android-based smartphones, while the majority of UIUC [USA] students had iPhones from Apple" (Lee and Song 2015, 156).

Lee and Song used a quantitative research method in the form of a three-part survey questionnaire: "Descriptive statistical analysis helps the reader compare the responses from the two universities to the same questions, and the results are presented in percentages and actual numbers" (2015, 155).

Even though their research method and focus are different, Lee and Song's research is relevant to the findings and discussion of this study, which also examine the mobile phone habits and attitudes within two distinct student participants from different cultural backgrounds.

Concluding, Lee and Song claim that "this comparative study explored some fundamental aspects of mobile information-seeking behavior among US and Korean students, and the results will help researchers and practitioners to develop hypotheses for conducting further research and creating new service profiles for mobile users" (2015, 160).

Another research group, **Park and Mo Jang** claim "there has been the conspicuous absence of empirical endeavors that systemically examine mobile-related knowledge and skill" (2014, 297), and thus in their research study from 2014 they investigated mobile privacy skills and knowledge of young African American adults. They used mixed method research (survey analysis and interviews with observations) studying a small group of students (60) "from a historically black college and university (HBCU) campus in a major metropolitan area in the US" (2014, 298). Particularly exciting findings from the survey analysis are that "42.4% of the participants also mistakenly believed that it is illegal for smartphone providers to collect locational data based on their mobile use" (2014, 299). In addition, "over half of them (57.6%) indicated that they rarely restricted the use of location-based mobile service" (2014, 300). Results from the interviews portrayed "the extents of the lack of knowledge and skill were confounded by basic feature confusion, functional misunderstanding … [An in-depth] interview, in fact, shed light on how various forms of new digital data surveillance on mobile platforms were misunderstood." (2014, 301).

In their conclusion, the authors give several excellent recommendations on how the FCC (Federal Communications Commission) should support mobile privacy awareness and education. These are " (1) Federal training aid in local level digital literacy programs (2) Standardization of mobile-apps privacy functionalities, and (3) Targeted awareness program for young users, especially from minority segments"(2014, 302). It will be interesting to see whether any of the authors' recommendations have been adopted within the US. Moreover, the time between this research and their study (about five years) may have had a positive influence on mobile privacy awareness and knowledge.

An article by **Shklovski et al.** (2014) is one of the few to study people's feelings and emotions about data tracking and personal data leakage from apps. They designed a two-phase study, with the first comprised of semi structured interviews with six participants from Denmark and seven from Iceland. As part of these interviews, people were asked about their "attitudes and beliefs about data privacy" (2014, 2350). To gain a more international as well as broader understanding, Shklovski et al. then followed up these interviews with an online survey recruiting international participants utilizing opportunity sampling. Here they also included a set of questions focusing "specifically on attitudes towards data collection and management by smartphone apps" (2014, 2351). The researchers also take a closer look at the notion of "creepiness" associated with data tracking and leakage. Shklovski et al. suggest "that designers of apps and their data sharing policies need to confront the nature of creepiness head-on. For this, we need a practical theory of creepiness, its varieties, and its temporalities, e.g.: Does creepiness fade over time with familiarity, and if so, what replaces it?" (2014, 2355). Similar to other articles discussed (see for example (King 2012)), they use as their theoretical privacy framework Altman's concept of personal space and territoriality and Nissenbaum's contextual integrity model.

In their discussion, Shklovski et al. somewhat refute the privacy paradox notion, and argue it "may obscure, complex dynamics around technology use and data disclosure" (2014, 2352). Instead, they suggest using Altman's learned-helplessness, which is "repeated invasions into a persons' privacy and a conviction that there is no recourse can result in learned helplessness [23,30] when people stop responding to invasions"(2014, 2354).

There is one thing Shklovski et al. could have considered a bit more – even though their online survey was answered by "respondents [who] lived in Denmark (43%), Iceland (20%), USA

(20%) and Sweden (10%)" (2016, 2351), the findings and discussion did not touch on cultural difference, despite the study's admission that they are relevant: "Questions of personal space and privacy are clearly culturally dependent, and from, e.g., Chinese or Global South perspectives smartphones may have very different meanings" (Footnote 1, 2014, 2347). Even further, they argue in their conclusion:

> Cultural norms change over time, subject to a great many short- and long-term forces, technical, economic, social, and legal. Acceptable entertainment app behavior in 2013 will likely be different than in 2023. This will not eliminate creepy experiences, but will change the conditions under which they are encountered. (2014, 2355)

Already by 2013, the researcher **Cushon** called for best practices in privacy education on mobile and social technologies. She gained her understanding of the importance of the topic through her work as an academic librarian. In her article, she addressed the benefits and risks of embracing mobile technologies and social media, which "have changed our perceptions of privacy and security, but, like many users, I am rather lackadaisical about protecting my information in these areas" (2013, 92). To resolve this, Cushon explained how she plans to become a privacy-conscious role model, both in her mobile technology and social media usage. Supporting her claim that it would be effective to educate students about privacy issues on social media and mobile technologies, she stresses that "students are at least partially aware of the risks to their privacy, even if they do not take steps to protect themselves. This means that students are highly educable in this regard" (2013, 95).

Cushon's first goal is to educate librarians through webinars, discussions, and working groups in order to create a pro-privacy learning environment. Furthermore, she suggests that libraries should create mobile technology policies within their institutions, as this will showcase responsible and knowledgeable behavior concerning privacy. Concluding, she reiterated how privacy education on mobile technologies and social media should be an integral part of academic librarians' responsibility, as it will help to cross-fertilize privacy awareness among students.

Overall, Cushon's article is more of personal essay or practical experience article than an in-depth research article. Nonetheless, the importance she places on mobile privacy education for librarians and students is commendable.

In 2012, **Cyrus and Baggett** (2012) explored the relationship between libraries, privacy, and mobile technologies and how user privacy issues challenge librarianship. Starting with defining privacy, they point out that within the library literature, there is a lack of a clear and precise definition for it. To address this, they look at prominent privacy definitions by scholars such as Warren and Brandeis (1890), Westin (1967), and Ware (1977). Their preferred definition is Westin's and they chose to focus "on how an individual controls access, use, and communication of information…" (2012, 286). Later the authors give a brief overview of American librarianship and privacy, noting how the "…'techie' role coupled with the rapid progression of technology opened new avenues for the librarianship in the area of privacy" (2012, 287). Then Cyrus and Baggett bring up the contradictory behavior of Americans regarding privacy.

On one hand, people are concerned about increasingly losing their right to privacy while at the same time trading personal information for free services. Here the authors point out how in America too much digital privacy rights for users are perceived as a threat to hinder technological and economic development. However, they also emphasize how, despite this popular sentiment the "importance of privacy is that, regardless of the technology, users have the right to know what information about them is available and what it is being used for" (2012, 289). The most significant part of this article is the two last paragraphs.

First Cyrus and Baggett depict how mobile technologies, such as apps, geolocation, facial recognition and augmented reality can infringe on privacy and how "it remains essential that we not overlook potential problems represented by these innovations" (2012, 289). They then link it to librarianship by providing three recommendations for librarians to actively influence the discussion on mobile technologies and privacy (2012, 292). The first is to stay informed on mobile technologies and privacy, be it on legal and business matters or keeping ahead of trends and developments. The second is to educate library users on mobile technology and privacy issues via different channels, such as library marketing and instruction: "A short section, or even a few sentences, on mobile technology and privacy could be added to almost any library orientation to raise awareness of the potential for harm and to exhibit safe or best practices that users may want to adopt" (2012, 294).

The final and third recommendation is to offer hands-on mobile privacy sessions where users could bring their own devices and have a dedicated privacy librarian expert to advocate for

privacy on a local and national level. Cyrus and Baggett bring up many vital and essential arguments on why privacy, and mobile technology knowledge should be considered a 21st-century expertise for future and current librarians.

King (2012) applies "two theories of privacy to examine smartphone users' concerns with other people and applications accessing the personal information stored on their smartphones" (2012, 2). The two theories are Nissenbaum's notion of "privacy as contextually appropriate information flow" (2012, 5) and Altman's "privacy as boundary regulation" (2012, 5). King's article's research method relates to this study as it uses a qualitative method in forms of interviews as well as card sorting. Also similar to this research methods, she allowed participants to use their smartphones: findings are based on eleven iPhone users versus thirteen Android phone users. Using quotes, she elicits some crucial findings on phone habits, such as "I am extremely addicted to my iPhone. I use it all the time" (2012, 5), and an attitude toward lending a phone to a friend or family member as opposed to a stranger, "I'd say it'd be better off in the friend's hands than the stranger's hands, although personally, I would keep my phone away from either" (2012, 6). Or about apps and trust: "When you engage in a relationship with this phone, with all these applications and what not, there's an understanding here that you are going to respect me and I'm going to respect you back" (2012, 7). And apps and reviews: "I want them to review because I want them to protect me from unscrupulous data collectors" (2012, 8).

Drawing back her findings to Nissenbaum's privacy theories, King confirms contextual privacy as a reality, as "users are open to granting contextually relevant access requests when the benefits are clear and circumspect when not. In particular, the proposition of sharing personal information with third parties when no contextual justification exists was non-negotiable for the majority of our participants" (2012, 12).

King proposes two valuable solutions on how to strengthen mobile privacy. These are first, implementation of privacy by design, thus removing the burden of mobile privacy complexity (see also Hartman's article (2011) discussed below) away from the user and second demanding uniformity and clearer privacy policy design from all mobile app stakeholders.

Hartmann's (2011) theoretical chapter describes mobile privacy from different perspectives. In the introduction, she looks at different scholars' understanding of mobility and privacy. Like

other authors already reviewed in this chapter, she defines privacy with reference to definitions by Warren and Brandeis, and Westin. Looking then at Arendt's definition of privacy versus being public or in public, Hartmann argues that "privacy is closely related to publicness, and they both depend on each other; secondly, privacy is related to both physical and locational questions as well as to informational ones" (2011, 194). Raising the question of what mobility is and how it can possibly be defined, she draws upon John Urry's five forms of mobility: corporeal travel, physical movement, imaginative travel, virtual travel, and communicative travel. According to Urry, all of them can exist in a symbiotic way. Hartman takes these "interdependent forms of mobility into account, and assuming that they are all relevant to the mobile privacy question, it becomes clear that privacies are related not only to people but also increasingly to objects and applications" (2011, 195). Next, Hartmann depicts the technical and philosophical context of mobile privacy. She illustrates different technical solutions by different scholars such as Perkins (Arkko, Perkins, and Johnson n.d.), Beckwith (2003), and Singh (2011) summarizing her interpretation as "our technological takes on privacy and mobility, we find an emphasis on the provision of opt-in rather than opt-out mechanisms" (2011, 197). Moving onto the philosophical perspective of mobile privacy, Hartman then highlights how in recent years privacy has been strongly associated with different contexts by different scholars such as Boyd and Nissenbaum. Hartman agrees that all "the aspects mentioned by Nissenbaum (2010), such as roles, relationships, and norms, may play a role in how users define privacy in given contexts." In the final subsection of the chapter, Hartmann tries to define mobile privacy through three different approaches. In the first, she places privacy and mobility on a spectrum matrix with the possibilities "to enable both users and researchers to locate different actions, situations, and contexts on this spectrum/matrix and thereby enable awareness of different variations and implications" (2011, 200). For the second, she suggests a "seemingly simple matrix of who/what/how/where/when of mobile privacy (or rather mobile privacies …)" (2011, 200). While this is not her preferred definition, it leads her to the third rather complicated definition, which is a combination of Urry's five forms of mobility and technical and philosophical aspects of privacy Hartmann has discussed. These five privacies are corporeal privacy, physical privacy, imaginative privacy, virtual privacy, and communicative privacy. In this definition, communicative privacy as a subset of mobile privacy is "protection related to

interpersonal communication on every level and with every medium. Here, too, the basis builds on technological questions and answers" (2011, 201).

Even though Hartman's article is theoretical and lacks empirical proof, it is one of the few articles that draw upon the philosophical, technical aspect of both privacy and mobility. Moreover, it is one of the few articles offering a definition of mobile privacy. Her article also highlights the complexity of mobile privacy: there is no single understanding of it, and neither is there a single solution on how to protect it.

3.10 Summary of Scholarly Context

In this literature review a summary of the literature relating to privacy, culture, ethnography, mobile security, and mobile privacy is provided. Within the research available, there was little literature covering qualitative in-depth mobile privacy research, and there was no qualitative study investigating mobile privacy attitudes and behavior in a cross-cultural setting. This dissertation addresses this research gap.

4. Research Method: Ethnography

4.1 Overview

The previous chapter reviewed ethnography. In this chapter ethnography as a qualitative research method will be only briefly discussed, since more emphasis is given to this study's particular ethnographic concept, which is thick description.

Next the research instrument is described, which includes pre-instrument design considerations, interview components, and (in greater detail) the interview guide for Fieldwork 1 and 2. Following Fieldwork preparations such as research ethics, the recruiting process as well as pilot testing for Fieldwork 1 and 2 are described. In conclusion quality standards for this study are presented.

4.2 Ethnography: A Qualitative Research Method

Overall the literature chapter has highlighted the need for qualitative research as a method to research mobile privacy. Flick remarks that "Qualitative research is oriented towards analyzing concrete cases in their temporal and local particularity and starting from people's expressions and activities in their local contexts" (2009, 21).

Ethnography as a qualitative research concept is:

> not about what is sometimes referred to as "giving voice" to participants. It is about providing an illuminating account for which the researcher is solely responsible. At the same time, since ethnography is a social activity, it does not occur in a vacuum, and it is likely that many other people, including but not limited to the direct participants, will have a stake in what comes out of the research, and in how things are represented. (Heller 2009, 251)

According to Bell ethnographers use a variety of methods to investigate cultures, such as participant observation, interviews, and reviewing historical and current documents. (Bell 2006, 16–17)

4.3 Thick Description as Ethnographic Method

This dissertation's ethnographic understanding is influenced by Clifford Geertz, who was one of the most forefront theorists and practitioner which "has produced the highly specialized field of 'ethnoscience' on the one hand and 'thick description' on the other (Sanday 1979, 533). Geertz is known for popularizing the "thick descriptive" approach to ethnography. Geertz emphasized that:

> doing ethnography is establishing rapport, selecting informants, transcribing texts, taking genealogies, mapping fields, keeping a diary, and so on. However, it is not these things, techniques, and received procedures that define the enterprise. What defines it is the kind of intellectual effort it is: an elaborate venture in, to borrow a notion from Gilbert Ryle, 'thick description'. (Geertz 1973, 6)

Thick description as an ethnographic approach might seem ambiguous, or even confusing to some researchers. For example, J.G. Ponterotte points out that:

> the Subject Index of virtually every major textbook on qualitative methods published during the last three decades includes one or more entries under either "thick description," or "description, thick" (Bogdan & Biklen, 2003; Creswell, 1998; Denzin, 1989; Denzin & Lincoln, 2005; Lincoln & Guba, 1985; Marshall & Rossman, 1999; Patton, 1990, to name but a few). Despite the widespread use and acceptance of the term "thick description," in qualitative research, there appears to be some confusion over precisely what the concept means (Holloway, 1997; Schwandt, 2001). (Ponterotte 2006, 538)

He then continues to clarify:

> Thick description captures the thoughts and feelings of participants as well as the often complex web of relationships among them. Thick description leads to thick interpretation, which in turns leads to thick meaning of the research findings for the researchers and participants themselves, and for the report's intended readership. Thick meaning of findings leads readers to a sense of versimilitude [sic], wherein they can cognitively and emotively "place" themselves within the research context. (Ponterotte 2006, 538)

As the focus of this study is to investigate and compare approaches and opinions about mobile privacy from an intercultural ethnographic viewpoint, two different languages, German and American, play a vital role in this study's thick narrative. Language and culture are closely intertwined – "If we want to study language, we have to consider its relationship to culture. If we want to investigate culture, we must research language" (Copland and Creese 2015, 13). Therefore, this bilingual study's thick descriptive approach analyzes the linguistic expression

of its participants closely, as "language is not only a model for studying other symbol systems, it is the primary channel by which analyses are communicated" (Manning 2001, 15). Therefore, participants' attitudes, defined in the research question as their feelings and established perceptions, are expressed by exposing specific linguistic highlights

4.4 Research Instrument

The research instrument design went through several stages that corresponded with the writing and rewriting of the thesis proposal. And that initial work was important, since "the research questions shape the selection of a place and a people or program to study" (Fetterman 2010, 35). The following subchapters explain the different phases.

4.4.1 Pre-Design Phase

Two issues had to be addressed before the data collection was to be conducted:

- **Informants:** library and information science students were chosen as informants, since a) privacy education might be part of the curriculum in information science departments, and b) current students grew up using mobile technologies. They might therefore have been exposed to mobile learning as part of their education. The thesis advisor recommended examining ten American and ten German students.
- **Access:** with the help of the doctoral advisor access to students from Berlin School of Library and Information Science at Humboldt University Berlin (*Humboldt Universität zu Berlin)* and the School of Communication and Information Sciences (SC&I) at Rutgers University was gained. Both schools are part of the iSchool organization[9] and are comparable in the size of their enrollment as well as their educational mission and vision.

[9] iSchool stands for "Information School". iSchools study the opportunities and challenges of information management. This includes data science and management, library science, archives and digital curation, and technology design for the purposes of information access and management. See https://ischools.org/

4.4.2 Components

Different data collections components were integrated into one interview instrument.

These were:

- **Demographic pre-interview questions**: the first part of the interview schedule was a short demographic survey.
- **Experiment**: Several scholars such as Umlauf, Fühles-Ubach, Seadle (2013) and Lesorogol (2005) confirmed that "experimental methods provide a novel way to triangulate with ethnographic methods such as observation, interviewing, and surveys. Mainly when the evidence from ethnography is mixed, experiments have the advantage of focusing on particular types of behavior and enabling the researcher to observe numerous individuals faced with the same behavioral choice" (Lesorogol 2005, 129).
- **Interviews**: Semi-structured interviews were used since they "combine the flexibility of the unstructured, open-ended interview with the directionality and agenda of the survey instrument to produce focused, qualitative, textual data at the factor level" (Schensul, Schensul, and LeCompte 1999, 2:149).

  Furthermore, Fetterman (2010, 40) points out that semi-structured interviews are ideal for answering specific research questions and for comparative studies.
- **Participant observation**: Denizen explains that "as a field strategy" participant observation "simultaneously combines document analysis, interviewing of respondents and informants, direct participation and observation, and introspection" (1989, 157–58).

4.5 Interview Schedule Fieldwork 1 and 2

4.5.1 Fieldwork 1

The interview schedule included a pre-interview survey, three guided parts, and a non-guided debriefing section. In the following the interview schedule is explained:

Part A: Demographic Questionnaire. Pre-interview students were asked to fill out a short demographic survey (Appendix 1, Appendix 2). Here some questions were specially included to be used as interview preparation or for the "icebreaker" and were not for analysis.

Part B: Questions about your smartphone and how you use it. (Appendix 3, Appendix 4)

The goal for part B was to assess informants' habits and attitudes in relations to their smartphones.

General questions (in two versions: American and German questions) about students' smartphones included the following:

> What kind of smartphone do you have?
> How long have you owned [sic] current phone?
> Is there a reason why you choose this particular model or phone?
> Alternatively, why did you choose this phone?

Some questions investigated participants everyday smartphone habits more exclusively.

> What do you do with your phone? Can you tell me a bit about your phone usage habits? What do you use it for? What are things you use it for a lot, and what are things you rarely do with it?

Asking participants about their favorite app was done with the purpose of returning to it as part of question in Part C.

> You just told me your five top apps, which one would you say is your absolute number 1? Your most favorite app? Or the one you use the most? Why?

Part C: Experiment and observation. (Appendix 5, Appendix 6)

The primary objective was to watch and observe how participants use apps and their smartphones in relation to mobile privacy. This was also the more apparent observational part of mobile privacy behavior and attitude. For participants, it was the most practical and hands-on section.

Finding the right app proved not to be an easy task. The app needed to be relatively simple and it needed to be available in the German and American Google Play store (Android) and the App Store (Apple). After some research, privacygrade.org (*PrivacyGrade*, n.d.)[10] was chosen, see homepage in Figure 2.

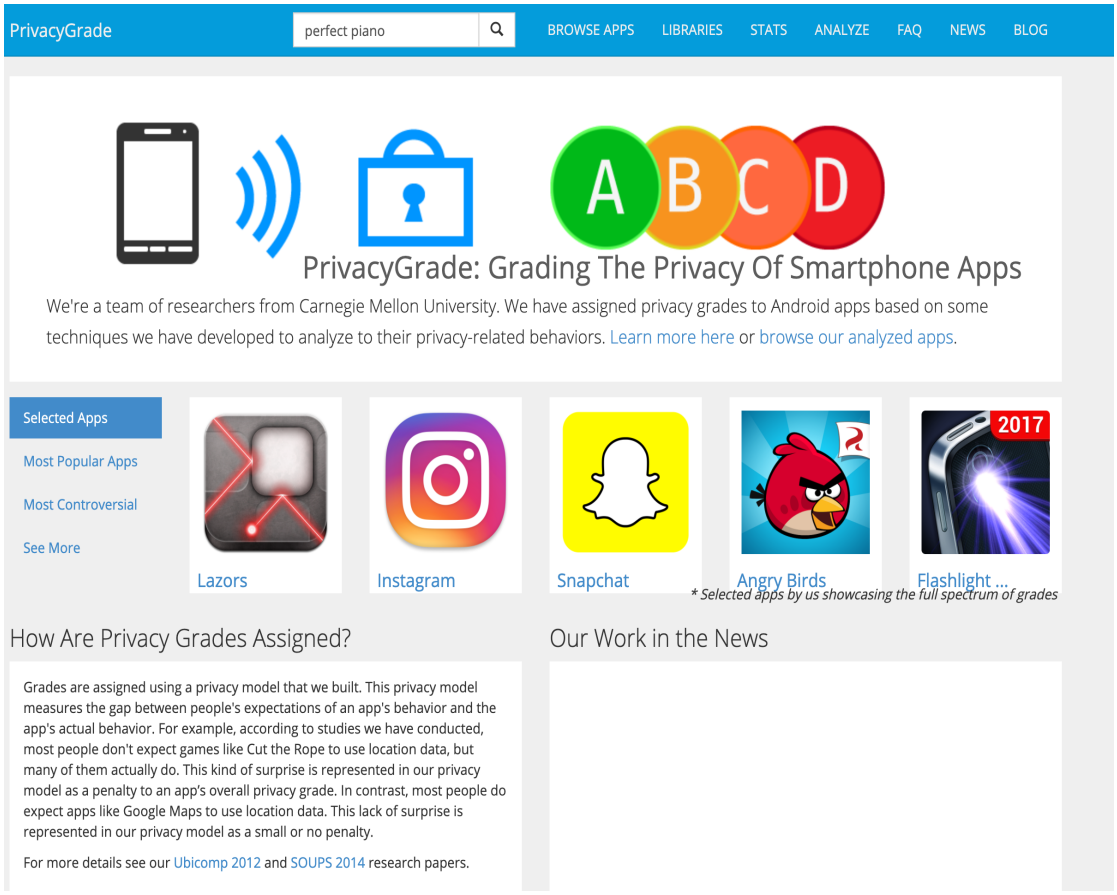

Figure 2 privacygrade.org homepage.
Accessed January 20, 2020. http://privacygrade.org/

[10] The website privacygrade.org was built by a team of researchers who were part of a research project at Carnegie Mellon University, primarily part of the CHIMPS lab. This website rates many different apps; however, due to the nature of Apple's restricted app ecosystems, only Android apps are rated. According to the site, grades from A to D "are assigned using a privacy model that we built. This privacy model measures the gap between people's expectations of an app's behavior and the app's actual behavior. For example, according to studies we have conducted, most people do not expect games like *Cut the Rope* to use location data, but many of them actually do. This kind of surprise is represented in our privacy model as a penalty to an app's overall privacy grade. In contrast, most people do expect apps like *Google Maps* to use location data. This lack of surprise is represented in our privacy model as a small or no penalty" (*PrivacyGrade* n.d.); you can read more about the site's privacy model at Lin et al. (2012) and Lin et al. (2014).

Several different apps were tested during pilot testing of this research project and in the end the app Perfect Piano[11] was selected. Although the app seemed like a simple music game app, at the time of data collection for Fieldwork 1, privacygrade.org had given it a C, which means there is a perceived discrepancy between what users expect the app to have access to (for example only network access) and to what the app actually has access to (including a contact list and photos).

The first question queried participants familiarity with privacy management options on their smartphones:

> Let's look at your phone now. Do you know where the privacy settings on your phone are? Like settings to protect your personal data/and or information? Can you show it to me?

One of the questions was both an inquiry and an observation of a student's behavior and attitude while downloading and trialing a new app:

> I am going to ask you now to download an app onto your phone. I would like to tell you two things beforehand 1) You can delete and uninstall the app immediately after the interview is over, and 2) If you do not want to use your personal phone, I can give you either my Android phone or my iPhone. Okay – so that is the app [give the note with the name of the app to the student]: Perfect Piano. So just download it and tell me a bit about how you usually do that.

During the instrument preparation time (in fall 2016) WhatsApp, a popular messenger service had received attention in the media for updating its privacy policy and starting to share data with Facebook[12] (Fox-Brewster n.d.) Therefore Question 23 American version (24 German version) probed whether students were aware of this issue and whether it had affected their mobile privacy behavior and attitude.

Part D: Questions about mobile data protection and mobile privacy. (Appendix 7, Appendix 8) In the last part of the interview the questions were more abstract and philosophical, to place participants' thoughts on mobile privacy and mobile data protection in a greater context.

[11] Perfect piano, an intelligent piano simulator design for phones and tablets. With in-built natural piano timbre, this app can teach you how to play the piano and amuse you at the same time!"(*Revontulet Soft, Perfect Piano, Walk Band, Nora, Revontulet Studio* n.d.)

[12] In 2014 Facebook bought WhatsApp for 19 Million Dollars.

The intention here was to get to know how participant define privacy in their own words:

I am going to ask you some more general questions now:
Can you tell me what privacy is or what privacy means to you?

The final question sought to find out students' thoughts on personal information and data transparency and this researcher asked:

Okay – you made it – this is the final question. So … is it actually okay with you that all our personal information or data that we have on our smartphones is transparent? Like is it okay for you, let's say that you and I - or we as people as humankind and all our information and personal data is transparent? As if we made out of glass … Like I don't care, I don't mind sharing everything, and everybody can know everything about me … Or do you think that this is not good and things should or need to change?

Part E: Debriefing section: This section was more informal, and not part of the semi-structured and scripted interview schedule. Time permitting, participants and the researcher discussed Android or iPhone privacy and security settings. Additionally, students were briefly introduced to the privacygrade.org website and presented with Perfect Piano's grade. This demonstration often elicited critical remarks from students. Sometimes students requested a search of their favorite app to reveal its grade. In return, this often led to more discussion on the topic.

In some cases, interviewees were introduced to two privacy apps. The first one was PrivacyProxy[13] (*PrivacyProxy - Privacy Reimagined* n.d.) which was released by the same research lab that developed and maintains the privacygrade.org website as a component of a research project. The second app was Privacy App, by Snoopwall (LLC n.d.).[14]

[13] The app states that it "helps you protect your private information by giving you control of what information is sent out from your device. Privacy Proxy is unique as it even filters the personal app identifiers if you choose to do so. The PrivacyProxy app is developed as a joint effort by the research team of CHIMPS Lab and Synergy Lab at Carnegie Mellon University in Pittsburgh" ("PrivacyProxy - Apps on Google Play" n.d.).

[14] Privacy App monitored apps permission such as location, file, settings and more. It is no longer available

4.5.2 Fieldwork 2

When the Facebook privacy data scandal occurred in March 2018,[15] this study was still in the data analysis stage. Hence the opportunity was taken to conduct a small follow-up study.

The interview schedule was as follows:

Question 1, an extemporaneous question meant as an icebreaker.

The objective of the two parts that made up **Question 2** was to gauge if or whether people had heard about the Facebook scandal. They were chosen to investigate participants' feelings and behavior about the data breach scandal.

Question 2: As a result of our conversations last year, do you have a different awareness about the Facebook scandal?

a. How does it make you feel about privacy on your smartphone?
b. Has it affected any of your privacy behavior?

The intention of the next two questions was to measure interviewees' awareness of the European General Data Protection Regulation and knowledge of its implications:

Question 3: In the last few months, have you received or noticed any updated privacy policies? (e.g., via email or for some of the apps or online services you use)?

a. Did you read any of the updated policies?
b. Any idea why you received those policy updates (GDPR awareness question)?

During Fieldwork 1, some students brought up mobile privacy in the context of who is or should be accountable and responsible for it. Hence Question 4 enquired:

Question 4: Who do you think should be primarily responsible for protecting the privacy on your smartphone? I am going to give you a few options:

a. Government
b. Companies
c. Or yourself

The final question addressed mobile privacy education, awareness, and advocacy of and for consumers.

Question 5: Do you think education on privacy, including education about your smartphone privacy, should be done in schools, for example, high schools or primary schools or later through university courses, e.g., if you do your bachelor's or master's?

[15] see https://www.nbcnews.com/tech/tech-news/facebook-s-2018-timeline-scandals-hearings-security-bugs-n952796

4.6 Fieldwork Preparations

4.6.1 Research Ethics

When researching with human subjects, it is crucial to follow ethical research practice, and it is "an essential and ongoing component of ethnographic practice" (Brewster, 2016). At the Berlin School of Library and Information Science, ethical research is upheld by the board of the Fakultät (faculty), which acts as the guiding board. For this study ethical approval was obtained by submitting a research approval letter to this board. (Appendix 9)

Fetterman points out, "Ethnographers need the trust of the people they work with to complete their task" (2010, 145). To uphold research integrity, study participants were from the onset of the recruitment process treated with openness and honesty. The call for participation via emails informed interested participants about the topic, anticipated time, and explained informed consent. (Appendix 10, Appendix 11) Moreover, at the beginning of each conducted interview, an informed consent document (Appendix 12, Appendix 13) was explained and then signed by participating students and the researcher.

Experience from previous research studies had taught this researcher that it was easier to recruit participants if there is a reward included. Participants received a small amount of monetary compensation: 10 euros for German participants and $15 for US participants cash, or the same amount as an Amazon gift certificate.

4.6.2 Recruiting Fieldwork 1

Recruitment for German study participants was done via email to Berlin School of Library and Information Science list server at the beginning of December 2016. The first round of recruitment yielded some positive feedback and five interview dates were organized. Yet, since the Berlin School of Library and Information Science went on holiday break at the end of December 2016 until the beginning of January 2017, timing was not ideal. Therefore, the original invitation was resent on January 4, 2017, via the institute's list server. Furthermore, the student council[16] was approached to distribute the invitation via their email contact. Due to this follow-up call, all participants were recruited by mid-January 2017.

[16] see https://www.ibi.hu-berlin.de/de/studium/fachschaftsinitiative

The recruitment of the American students started at the beginning of February 2017 and by beginning of March 2017 ten American students were found.

All participating students were emailed the demographic questionnaire a few days before the interview date via email.

4.6.3 Recruiting Fieldwork 2

For the follow-up study, four participants (two American students and two German students) were chosen. Not all participants from Fieldwork 1 were suitable for this study, because they had to have been identified as active Facebook users.

4.6.4 Piloting the Research Instrument Fieldwork 1 and Fieldwork 2

The preparation period for Fieldwork 1 and Fieldwork 2 included testing of the research instrument. According to Rothgeb, "The pilot test will also provide information about question comprehension, sensitivity, difficulty, and/or item nonresponse related to specific questions" (2008, 3). Both interview instruments were tested several times with German and American friends or relatives. As a result of these tests both interview guides were refined.
A Canon HD Vixia camcorder was used to record the interviews. Furthermore, as a backup precaution a MacBook Pro was used to audio record the interviews as well. In case some participants did not want to conduct some or all parts of the study on their own devices an inexpensive Android Motorola phone was purchased, and the researcher made her personal iPhone available.

4.7 Fieldwork 1 Germany and the US

The initial data collection was from January to March 2017. Interviews were conducted with students from Germany in Berlin in January 2017. The American data gathering occurred in New Brunswick, New Jersey, in March 2017. Observational reflections on Fieldwork 1 are described in subchapter further below.

4.8 Fieldwork 2 Germany and the US

Interviews for Fieldwork 2 were conducted in August 2018. This time the interviews were done remotely via Zoom video conference software. Interview perceptions are described in subchapter 5.3.2 Qualitative Data: Descriptive Background Information.

4.9 Quality Standards

There is a growing body of literature (see for example (Seale and Silverman 1997), (Flick 2009) and (Erlingsson and Brysiewicz 2013)) counterbalancing the debate on "whether qualitative research and qualitative methods can be truly considered 'empirical' and, therefore, adequately scientific" (Bhattacharya 2008, 254). The following illustrate the qualitative standards this study adheres to:

1. Ethical quality standards
2. Pilot testing of research instrument
3. Data Collection triangulation.
4. Validity of data via audio and video recording
5. Controlled and standardized transcription process
6. Computer-aided qualitative software and suitable qualitative text analysis method
7. Framing the results of Fieldwork 1 and 2 in relation to relevant scholarly literature.

4.10 Summary of Research Method

In this subchapter the methods and components to collect the data for this study was described. Scholarly articles, books, and advice from experienced ethnographers, fellow doctoral students, and information and library science peers were all utilized to keep research design limitations and research errors to a minimum. Perceived research limitation of the entire study will be addressed in chapter 12.

5. Data Analysis: Fieldwork 1

5.1 Overview

In this chapter the data analysis for Fieldwork 1 is explained.

First, the data preparation process, including field notes, interview transcription and screenshots is introduced. Then the data analysis procedure for quantitative and qualitative data is described, along with a detailed explanation of the data analysis method. Here the seven different phases are elucidated in detail, with Phase 4 and Phase 5 combined within one subchapter. Finally, a chapter summary is given.

5.2 Data Preparation

5.2.1 Post-Interview Field Notes

The first step in the data preparation process was to write up notes, labeled "first thoughts field notes." These notes helped to recap initial thoughts and notions, as well as striking occurrences for each interview. During the transcription process, these notes were of great value in helping recall memories of each study participant.

In order to keep them readily accessible and organized, all field notes were imported into MAXQDA Analytics Pro 2018 (MAXQDA), a Qualitative and Mixed Methods Research Software used for the data analysis process.

5.2.2 Interview Transcription

The transcription guideline (Appendix 14) for this study was modeled after recommendations by Dresing, Pehl, and Schmieder (2015) as well as Kuckartz and McWhertor (2014, 124–27).

All the interviews from Fieldwork 1 went through three stages of transcription to verify their accuracy. During the first pass, MAXQDA was used to analyze and transcribe the videos and to anonymize the informants' names to protect their privacy.

To protect participants' confidentiality, the original data was securely stored on the researcher's password-protected computer as well on an external password-protected backup hard drive accessible only to her. The abbreviation GS (*German student*) followed by numbers one to ten was designated for the German data, and the abbreviation AS (*American student*) followed by numbers one to ten for the American data.

During the second pass, the videos were rewatched via QuickTime software and screenshots were created, while simultaneously correcting any earlier transcriptions errors in MAXQDA.
During the third pass, transcripts were exported into Microsoft (MS) Word, and then the audio backup was used to listen to the interviews again. At this time, transcriptions were also formatted in MS Word and, if necessary, further corrections were made.
In the final step, MS Word documents were imported back into MAXQDA, this time a new document group was created.
Thus, original video transcriptions and the final transcriptions of the interviews were kept separate. Only the final transcriptions were used for the data analysis.

5.2.3 Screenshots

In order to visually analyze the interviews, screenshots of some of the study participants' videos were taken. To protect the participants' privacy, none of the screenshots displayed identifiable characteristics. They only depicted their mobile phone screens. In some instances, for example, if the images taken from the videos were not suitable, or if the informant did not use their phone screens to exemplify something, screenshots as a visual placeholder were re-created by the researcher. All relevant screenshots were exported as PDFs into MAXQDA.

5.3 Data Analysis Procedure

5.3.1 Quantitative Data

The quantitative data was derived from the demographic questionnaire as well as some responses from part B of the interview.
The following variables were entered into MAXQDA:

- gender (male or female)
- nationality (German or American participant)
- age
- degree (the final degree participants are pursuing: bachelor or master)
- class format (online, hybrid, in person)
- working besides studying (if participants have a part-time, full-time job or internship)
- hours per week if working besides studying

- working or studying before/something else (if students had a job before being a student)
- apprenticeship or occupational training in a vocational profession[17] (question only for German students

Additionally, the following informational variables taken from participants' responses were entered:

- tablet owner
- smartphone brand
- mobile operating system (OS) type
- year they first owned a smartphone
- smartphone adopter
- social network user

"Smartphone adopter" warrants a brief explanation: In the literature the technology adoption life cycle has been examined. The technology adoption life cycle is the adoption rate of new technological products in relation to their market shares; whereas "consumers fall into one of five basic classifications: innovators, early adopters, early majority, late majority or laggards" (Meade and Rabelo 2004, 667).

During the interviews, several participants considered themselves late smartphone adopters. Therefore, the question arose whether there was a correlation between smartphone adoption period and mobile privacy behavior and attitude. Moreover, whether statistical data for the smartphone adoption life cycle existed. Finding statistics and/or articles about the smartphone adoption life cycle proved very difficult. In the end, the date ranges are based on the following literature:

Number of Smartphone Users in Germany from January 2009 to 2018 (2018),
Number of Smartphone Users in the U.S. 2010-2023 (2019), and
The Diffusion of iPhones as a Learning Process (2013).

[17] see https://www.apprenticeship-toolbox.eu/germany/apprenticeship-system-in-germany/143-apprenticeship-system-in-germany

The succeeding definition smartphone adoption variables[18] are:

"early adopters" (2007-2009)

"early majority" (2010-2012)

"late majority" (2013-2015)

"laggards" (2016-present).

All aforementioned variables were then applied to the German and American transcription documents.

Table 1 shows statistical data after the variables were entered into MAXQDA**.**

		frequency	
		German students	American students
gender	male	5	6
	female	5	4
age	19-20	1	3
	21-25	2	1
	26-30	5	2
	31-35	2	0
	42	0	1
degree	bachelor	4	6
	master	6	4
tablet owner	no	6	7
	yes	4	3
mOS type	Android	9	3
	Windows	1	0
	iOS	0	7
smartphone adopter	early adopter (2007-2009)	1	3
	early majority (2010-2012)	4	3
	late majority (2013-2015)	4	3
	laggard (2016-present)	1	1
social network user	no	3	1
	yes	7	9

[18] None of the participants fell in the category innovator, thus it is not listed at all.

Table 1 German and American research study participants with frequency depicting number of students

5.3.2 Qualitative Data: Descriptive Background Information

An analysis of the interview preparation and interview methods follows. According to O'Reilly, "in ethnographic research, these descriptive data often take the form of what appears to be background data, but which are, in fact, beginning to answer the questions you started with" (O'Reilly 2012, 194).

5.3.2.1 Interview Setup German Data Collection

The researcher was able to conduct all the German interviews in person at the Berlin School of Library and Information Science, which was very convenient for the participants. Aided by two administrative assistants from the Berlin School of Library and Information Science, room 120 was reserved in advance.

The researcher usually arrived 30 minutes before each interview to set up the room and equipment and to ensure that the smartphones and MacBook Pro were connected to the institute's Wi-Fi.

In order to give herself time to focus on each participant and to properly prepare for the next interview, the researcher never scheduled more than two interviews per day.

5.3.2.2 Interview Setup American Data Collection

The gathering of American data took place at Rutgers's University New Brunswick campus. Initially the food court at the Student Center at Rutgers' New Brunswick campus was chosen as the interview locale. However, the food court turned out to be too noisy and disruptive for the interviews, and after the first two interviews to the rest were conducted in the quieter student lounge on the first floor.

5.3.2.3 Interview Observations: German and American Data Collection

The ethnographer in this study took great pains to build a rapport with study participants, since:

> An ethnographer's behavior in the field is usually his or her most effective means of cementing relationships and building trust. People like to talk, and ethnographers love

> to listen. As people learn that the ethnographer will respect and protect their conversations, they open up a little more each day in the belief that the researcher will not betray their trust (Fetterman 2010, 145)

Making participants feel safe and valued was a crucial component in gaining insights into their behavior and attitudes concerning mobile privacy. Pre-interview icebreaker conversations were an excellent opportunity to create a rapport with and earn the trust of the participants. In hindsight, this short talk about topics unrelated to the study was a key component, as it made the participants feel at ease. As a result, all participants felt comfortable to share sensitive and personal information about their phones and apps during the interview.
Before the interview, the German students were asked whether it was okay to say *Du,* the informal "you" in German, instead of the more formal *Sie*. They all offered and agreed to use the informal *Du*, which also contributed to a more intimate and personal atmosphere.

Overall there was excellent rapport between researcher and research subject during the interviews, which lasted between 45 minutes to 90 minutes.

5.3.3 Data Analysis Method: Thematic Qualitative Text Analysis

Data analysis does not take place in a vacuum. The decision to utilize Kuckartz (Kuckartz and McWhertor 2014) as guidance is based on:

1. "the fact that the research question is of central importance throughout the entire analysis process" (Kuckartz and McWhertor 2014, 160)
2. it is a rule-drive method that follows carefully collected data. Furthermore, and is a systematic scientific method, and thus maintains a level of quality standards and
3. offers in-depth instructions on how to conduct data analysis with MAXQDA.

Kuckartz proposes three different qualitative text analysis methods: thematic, evaluative, and type-building analysis.

For this dissertation thematic text analysis was chosen, since its theme-based analysis was perceived as the best way to compare findings between different cultures. The analysis was divided into seven different phases, which spanned from deductive phases to the inductive phase and concluded with an in-depth analysis of the results. Furthermore, the thematic analysis process was an iterative process, allowing for readjustment and movement from one

phase backward or forward if needed. (Note that the terms "categories" and "codes" are used interchangeably in the following phases.)

5.3.3.1 Phase 1: Initial Work: Highlights, Memos and Case Summaries

In Phase 1, each interview transcript was carefully read, and essential passages were highlighted. The MAXQDA memo feature was applied to annotate striking occurrences. To finalize Phase 1, all interviews were read in print, and short summaries using MAXQUDA's summary option were composed.

5.3.3.2 Phase 2: Main Thematic Categories

Main thematic categories were developed by reviewing the research question and the interview questions.

The research question yielded the following four thematic categories, which were classified as *deductive priori* categories. To keep them organized and useful as a working tool, an Excel document was created. The following table (Table 2) explains these four thematic categories:

deductive priori categories	**explanation of categories**
mobile privacy	Mobile privacy entails personal data and information being accessed or transferred onto mobile devices to device manufacturers, app developers, and other third parties - and if or how it is controlled and or protected.
mobile privacy behavior	Mobile privacy, plus how a study participant utilizes smartphones, apps, and mobile websites in their everyday life.
mobile privacy attitude	Mobile privacy in combination with the feelings, emotions, thoughts, positions and established perceptions of study participants.
mobile security	Mobile security is concerned with malware, viruses, spam, encryption, password protection on mobile devices.

Table 2 Deductive priori categories for Phase 2: four thematic categories

In the next study phase the interview questions were reviewed. This yielded the following seven different thematic categories (see Table 3):

deductive priori categories	explanation of categories
mobile phone habit	How participants use their mobile phones.
mobile phone attitude	Feelings, emotions, thoughts, positions, and perceptions linked to participants' mobile phones.
app experiment	How participants download and interact with the app used in experiment and observation part C.
WhatsApp	Whether participants use WhatsApp or were aware of WhatsApp and Facebook data-sharing and/or change of privacy policy (fall 2016).
privacy	Participants' definition of privacy.
data protection	Participants' definition of data protection.
personal information and data shared	Participants' thoughts on what personal information and data from a mobile phone is being shared with "Others." Moreover, who are these "others"/players/stakeholders? Participants' thoughts on what happens with all the collected information/data. Why? /Which purpose?
transparent human	Participants feedback on being a transparent human[19].

Table 3 Deductive priori categories for Phase 2: seven thematic categories add-ons

The established categories were tested by coding two student's transcripts (GS5 and AS5). This revealed that some categories required some more adjustments. *Privacy* and *data protection* were renamed to *privacy definitio*n and *data protection definition*, and further categories were added (see Table 4):

[19] In Germany a transparent human *("gläserner Mensch")* is used as metaphor for data privacy.

deductive priori categories	explanation of categories
mobile phone knowledge	What participants know about their phones, and how well participants know their phones.
app experiment privacy	How and what participants know about where the privacy settings on their phones are.
app experiment Perfect Piano	How participants download and interact with the app used in experiment and observation part C.
app experiment favorite app	How much participants know about the information/data and personal content their favorite apps have access to. Awareness about the privacy policy of their favorite app and/or the ability to find it.
mobile privacy definition	What participants think mobile privacy is.
mobile data protection definition	What participants think mobile data protection means.

Table 4 Deductive priori categories for Phase 2: adjustments of thematic categories

Then another test coding with GS5/AS5 and GS7/AS7 was performed.

Creating the initial thematic code framework proved challenging, as some of the central thematic categories were very closely related and also could be considered subcategories. Hence, the coding scheme was revised to establish parental hierarchical categories—a step Kuckartz does not include in his thematic approach.

Before moving onto Phase 3, the coding frame looked as follows (see Table 5):

mobile privacy	(**main** category)
mobile privacy attitude	(subcategory)
mobile privacy behavior	(subcategory)
mobile privacy definition	(subcategory)
mobile data protection definition	(subcategory)
personal information and data shared	(subcategory)
transparent human	(subcategory)
mobile security	(**main** category)
mobile phone habit	(**main** category)
mobile phone attitude	(**main** category)

mobile phone knowledge	(**main** category)
app experiment privacy	(**main** category)
app experiment Perfect Piano	(**main** category)
app experiment favorite app	(**main** category)
WhatsApp	(**main** category)
privacy definition	(**main** category)
data protection definition	(**main** category)

Table 5 Phase 3: parental hierarchical categories (bold) and subcategories

In the next step these categories were created as codes in MAXQDA

5.3.3.3 Phase 3: First Coding Process

During Phase 3, the codes were applied to the German and American data. While coding the experimental and observational part of the interviews, the original interview videos were rewatched via QuickTime to avoid overlooking any important details.

The following depicts a sample text passage with applied code "mobile phone habit" in Phase 3 (see Figure 3):

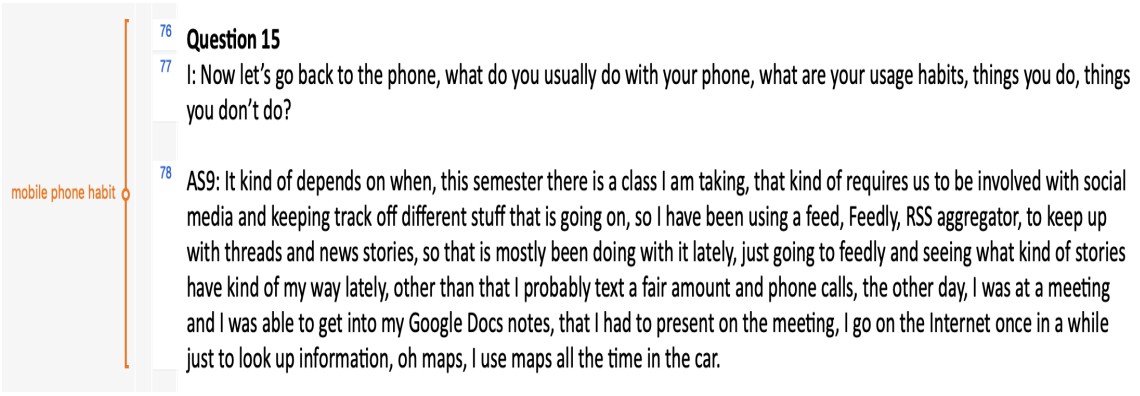

Figure 3 Phase 3: text passage with one applied code (pasted image)

As you can see in this example, the questions were included as part of the coded passages to make analysis easier.

During the first coding phase strict boundaries for some categories became indistinct. One solution was to allow for overlap within categories. To avoid errors, all coded documents were reviewed before moving into Phase 4. It was then noticed that the coding frame needed

another revision. Consequently, two more main theme categories and subcategories were added.

The following table (Table 6) depicts added deductive priori categories:

deductive priori categories	**explanation of categories**
lend mobile phone family/friend	Whether participants would lend their phone to a friend or family. And if so, for how long.
lend mobile phone stranger	Whether participants would lend their phone to a stranger, and what the stranger would be allowed to do.

Table 6 Phase 3: added deductive priori categories

The next table (Table 7) depicts the new subcategories, listed in bold in the middle column.

main category	**subcategory**	**explanation subcategory**
mobile phone attitude	**first smartphone**	Thought and/or feelings participants remembered about their first smartphone.
mobile phone habit	**daily usage**	Participants' guess as to how much they use their phones daily.
	computer versus phone usage	How students compare phone versus computer usage on average, either by amount of time or as a percentage.
	top five apps	Students' top five apps
	favorite app	Students' favorite app

Table 7 Phase 3: new subcategories (bold in middle column)

At the conclusion of Phase 3, some main themes were reorganized as subcategories of mobile privacy.

At the onset of Phase 4, the deduced categories were as shown in Appendix 15.

5.3.3.4 Phase 4: Compiling of Main Thematic Categories and Phase 5: Creation of Inductive Subcategories within Thematic Categories

MAXQDA text retrieval function was applied to filter each category for German and US participants. Next, the retrieved segments were exported into to MS Excel. A newly created MS Excel list was created to keep track of reviewed categories, marking them with a *No* if no inductive patterns and thus no further subcategories emerged. *Yes* was marked in the list if one or more inductive subthemes became apparent during the review process.

No inductive subcategories emerged for

- mobile phone knowledge
- privacy definition
- data protection definition
- WhatsApp
- app experiment favorite app
- mobile privacy definition
- mobile data protection definition
- personal information and data shared
- mobile security

The process to create inductive subcategories was as follows:

1. Using an open and reflective approach, inductive subcategories were noted in MS Excel. The researcher first created inducive subcategories for perceived easier main thematic categories, for example, mobile phone attitude. Then inductive categories for more complex main themes such as mobile privacy user attitude were created.
2. In the final step all created inductive categories were reviewed, revised as necessary, and then organized. Appendix 16 depicts the inductive categories.

5.3.3.5 Phase 6: Second Coding Process

In Phase 6, inductive codes were applied to the relevant text passages. It was then noticed that that the coding framework needed another further revision.

At the end of Phase 6, the *hierarchical thematic deductive, inductive* coding scheme, with numbers of applied codes was as shown in the following table (Table 8):

mobile privacy	239
mobile privacy attitude	239
convenience/ laziness	12
expressions/ words/ phrases non-verbal cues	108
data as trade	44
complacency/ learned helplessness	28
confusion unclear	38
Google/Facebook/Amazon/Apple	64
privacy policy	49
awareness/education	8
abstractness	11
law/ regulation/ control	15
ethical/moral/ philosophical/societal	7
surveillance	17
advertising	27
lend mobile phone family friend	20
breakage	2
personal device	8
lend mobile phone stranger	20
personal information	3
security risk	2
theft	8
value	6
mobile privacy definition	20
mobile data protection definition	20
personal information and data shared	24
transparent human	36
WhatsApp	21

(continuation of column 1)	
mobile privacy behavior	131
app experiment privacy	25
location service	22
app experiment Perfect Piano	86
reviews stars pictures	9
privacy policy	29
app experiment favorite app	28
mobile security	37
mobile phone habit	175
phone calls	10
favorite app	26
top five apps	24
computer versus phone usage	20
daily usage	22
mobile phone attitude	102
Android iPhone Other	24
value for money	19
first smartphone	23
mobile phone knowledge	45
privacy definition	21
data protection definition	20

Table 8 Thematic deductive, inductive coding scheme at the end of Phase 6 (main categories in bold)

5.3.3.6 Phase 7: Analysis by Summary Grids and Summary Tables

In the final phase, first MAXQDA's topic analysis summary was utilized. For each inductive and deductive category, the summary grid feature was used to write a synopsis of each participant.

The following image (Figure 4) shows an example of the subcategory *first smartphone* and summary notes for student GS10:

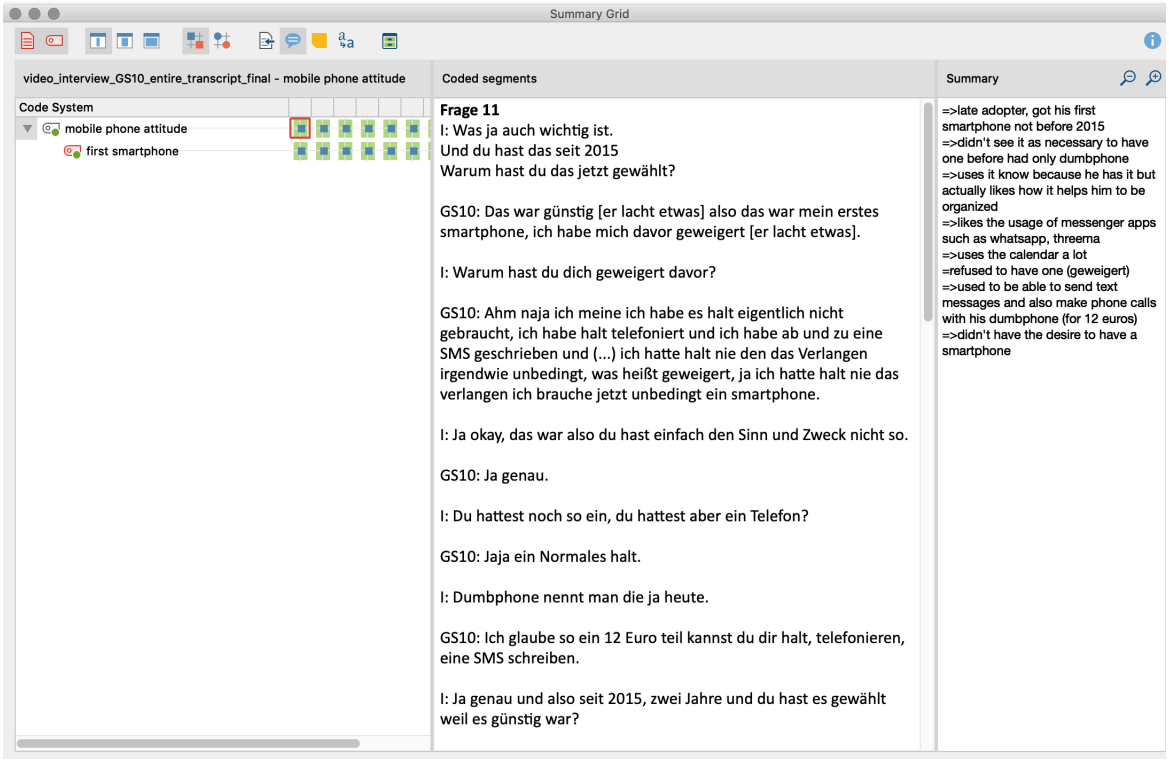

Figure 4 Phase 7: example of a subcategory,

here: *first smartphone* and summary notes (pasted image)

As next step, summary tables were created for all categories. This image (Figure 5) illustrates a summary table for all seven US students for the code *confusion unclear*:

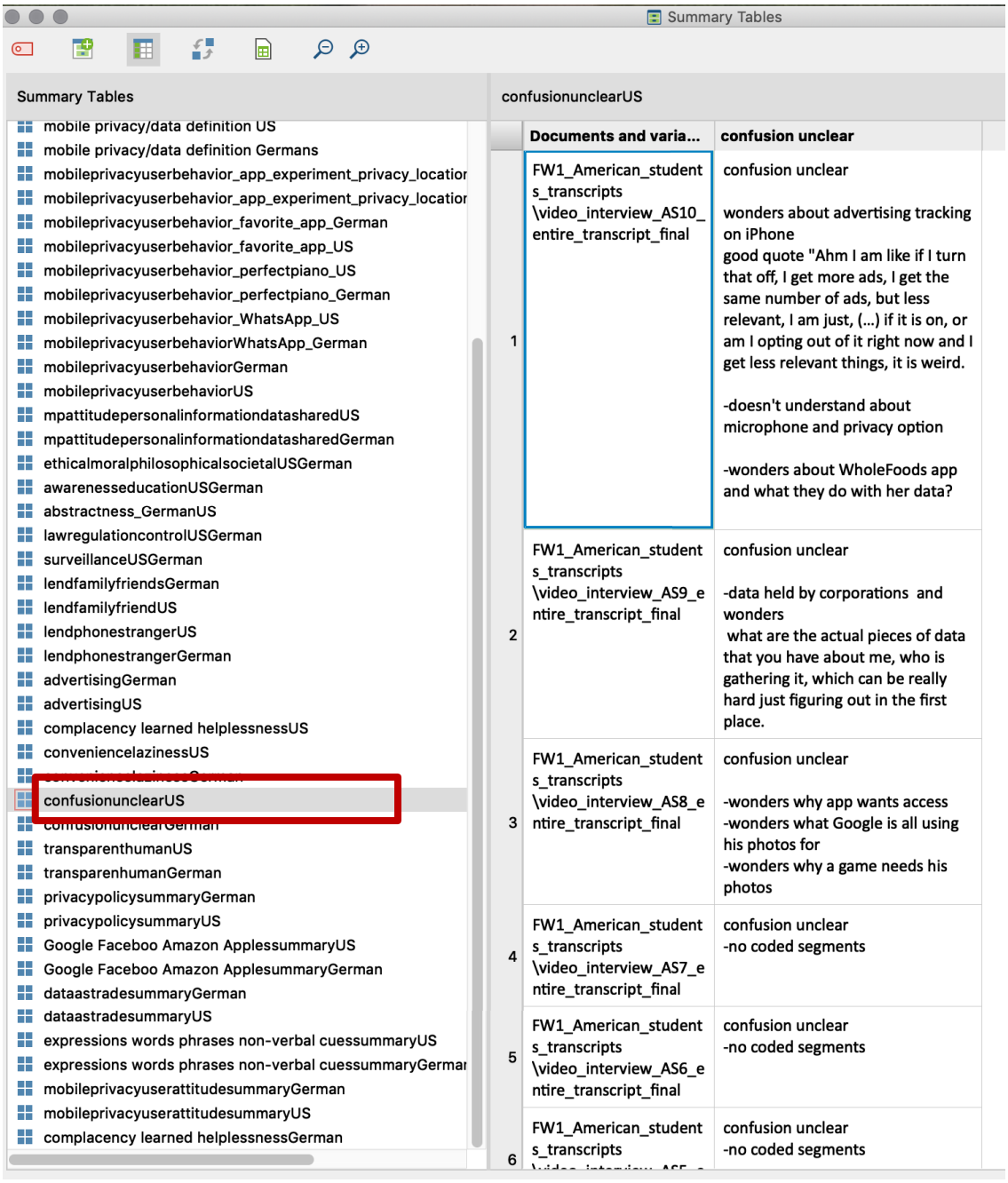

Figure 5 Phase 7: summary table for all seven US students for the code *confusion unclear* (pasted image)

Then all summary tables were exported into MS Excel and saved into folders labeled according to their themes.

After carefully reviewing these documents the decision was made to transform the analyzed data into a narrative by focusing on six major themes: mobile phone behavior, mobile phone attitude, privacy definition, mobile privacy definition, mobile privacy behavior and attitude, and mobile security. The mobile privacy behavior and attitude topic includes several

subthemes. Additionally, it became apparent during Phase 7 that the findings were highly suitable to be converted into composite narratives.

5.4 Summary

In this chapter the data analysis process has been described. The overall goal was to pull the data apart by coding it and then to reconstruct it into a narrative that answers the research question.

6. Data Analysis: Fieldwork 2

6.1 Overview

This chapter describes the data analysis for Fieldwork 2.

6.2 Data Preparation

In order to protect participants' confidentiality, the original interview data was securely stored on a password-protected external hard drive. Next, the data was exported into the existing MAXQUDA German American data analysis project created for Fieldwork's 1 data analysis. Then, the participants were anonymized by renaming them American Student Follow-Up 1 and 2 (ASF1, ASF2) and German Student Follow-Up 1 and 2 (GSF1, GSF2). After each interview, notes were written first by hand and then converted into MAXQDA memos at the beginning of the data analysis.

The following figure (Figure 6) depicts a sample memo for ASF2.

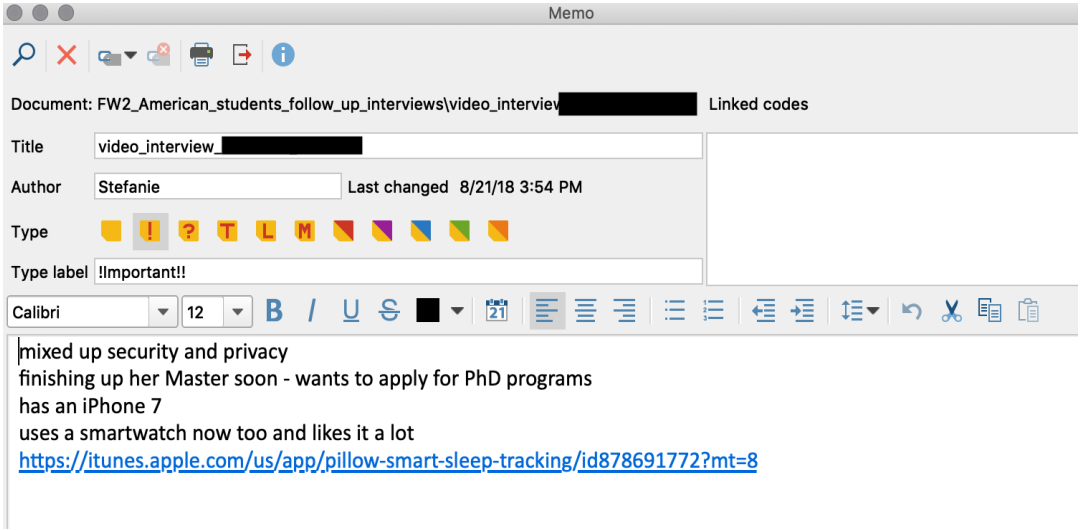

Figure 6 Fieldwork 2: Memo for ASF2 (pasted image)

Afterward, the interviews were transcribed using the procedures and rules described in chapter 5.2.2 Interview transcriptions.

Similar to Fieldwork 1, original video transcriptions and final interview transcription were kept in separate document folders.

6.3 Data Analysis Procedure

6.3.1 Quantitative Data

Reusing the quantitative data collected in Fieldwork 1, the following variables were entered for Fieldwork 2 via MAXQDA variables option: gender; nationality; age; first smartphone; smartphone-adopter; mobile operating system type.

The following table (Table 9) depicts the quantitative data:

Gender	Nationality	Age	First Smartphone	Smartphone Adopter	Mobile Operating System Type
Male	American	22	2009	Early Adopter (2007-2009)	iOS
Female	American	27	2013	Late Majority (2013-2015)	iOS
Female	German	26	2014	Late Majority (2013-2015)	Android
Male	German	30	2016	Laggard (2016-present)	Android

Table 9 Quantitative data: variables reused for Fieldwork 2

6.3.2 Qualitative Data: Descriptive Background Information

As a result of the rapport and trust established between interviewer and interviewee, the tone and atmosphere of all four interviews was relaxed, honest, and open.

An unusual occurrence in terms of location was observed with Student ASF1. He was grocery shopping during the interview and performed the interview via the Zoom video app on his smartphone. Aside from one interruption by a fellow grocery shopper (asking him if he knew where the tissues were), he remained focused and was able to fully participate in the interview.

On average, the interviews lasted 45 minutes, with the longest one taking 60 minutes and the shortest one running 25 minutes.

6.3.3 Data Analysis Method: Thematic Qualitative Text Analysis

As the thematic qualitative text analysis applied in Fieldwork 1 turned out to be a suitable method for converting the data in the findings chapter into a thematic narrative, the same process was used for Fieldwork 2. In the following chapters, the seven different phases will be explained in detail.

As previously done in data analysis for Fieldwork 1, Phase 4 and 5 are described within one subchapter.

6.3.3.1 Phase 1: Initial Work: Highlights, Memos

In Phase 1, all interview transcripts were carefully scrutinized, while relevant passages were highlighted and memos applied.

6.3.3.2 Phase 2: Main Thematic Categories

In Phase 2, thematic deductive categories based on the research question and the interview instrument were created. As mobile privacy, mobile privacy behavior, mobile privacy user attitude, and mobile security categories were already created as part of Fieldwork 1, they were reused in this context.

The following table (Table 10) depicts and explains the priori-deductive categories with Fieldwork 1 (Fw1) in parenthesis, indicating the reused categories:

deductive priori categories	**explanation of categories**
mobile privacy (Fw1)	Mobile privacy entails personal data and information being accessed or transferred onto mobile devices to device manufacturers, app developers, and other third parties - and if or how it is controlled and or protected.
mobile privacy behavior (Fw1)	Mobile privacy plus how a study participant utilizes smartphones, apps, and mobile websites in their everyday life
mobile privacy attitude (Fw1)	Mobile privacy in combination with the feelings, emotions, thoughts, positions, and established perceptions of study participants
mobile security (Fw1)	Mobile security is concerned with malware, viruses, spam, encryption, password protection on mobile devices.
Facebook scandal	Participants' various understandings about

	the Facebook scandal following the first interview (Fieldwork 1)
privacy policy update	Participants' awareness of updated privacy policies
read privacy policy	Reading of updated privacy policies by participants
GDPR	Participants' awareness and knowledge of GDPR
protection of mobile privacy	What entity should be in charge of privacy protection, including mobile privacy protection
education privacy	Participants' thoughts about when (age, school year, etc.) privacy education should begin

Table 10 Phase 2: Fieldwork 2: priori-deductive categories with reused codes from Fieldwork 1 (Fw1)

As utilized in Fieldwork 1, the coding scheme was divided into parental-hierarchical (main) categories and, if applicable, subcategories. The following table (Table 11) depicts the coding scheme, including main and subcategories:

mobile privacy	(**main** category)
mobile privacy attitude	(subcategory)
protection of mobile privacy	(subcategory)
mobile privacy behavior	(subcategory)
mobile security	(**main** category)
Facebook scandal	(**main** category)
GDPR	(**main** category)
privacy policy update	(subcategory)
read privacy policy	(subcategory)
education privacy	(**main** category)

Table 11 Phase 2: Fieldwork 2: parental hierarchical scheme (parental codes in bold)

Prior to Phase 3, the newly established categories were entered into MAXQDA.

6.3.3.3 Phase 3: First Coding Process

During Phase 3, the entire data set was coded. Overlapping of codes occurred again some instances. The following image (Figure 7) illustrates a text paragraph with applied overlapping codes *mobile privacy, Facebook scandal, mobile privacy user attitude, mobile privacy behavior,* and, highlighted in blue, the coded segment for *mobile security*.

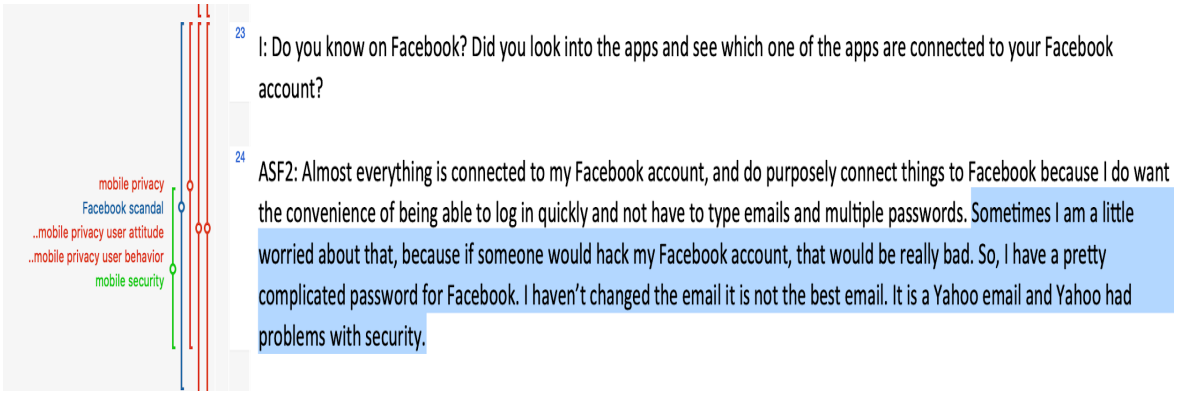

Figure 7 Phase 3: text paragraph with applied overlapping codes (pasted image)

After completing Phase 3, the entire data set was carefully reviewed to find any possible coding errors.

6.3.3.4 Phase 4: Compiling of Main Thematic Categories and Phase 5: Creation of Inductive Subcategories within Main Categories

During Phase 4, all passages were compiled via the main categories. Following this text retrieval, during Phase 5, inductive subcategories were created. Each main category was exported into Excel, and then the inductive review process began. The process was streamlined this time, since some of the inductive codes from Phase 5 in Fieldwork 1 reemerged and could be reutilized.

For some main categories, no inductive subcategories surfaced. These were *mobile security*, and *mobile privacy*, and the deductive subcategories *privacy policy update* and *read privacy policy update*.

Several subcategories were reused from the subtheme *mobile privacy user attitude*, and these are marked in the following table (Table 12) with Fieldwork 1 (Fw1).

main deductive categories	inductive subcategories	description of inductive subcategories
Facebook scandal	complacency/ learned helplessness (Fw1)	Participants believe they cannot change the situation and/or accept the current situation
Facebook scandal	mobile privacy behavior/ no_change_yes_change	Mobile privacy, plus how a study participant utilizes smartphones, apps, and mobile websites in everyday life, and whether they made behavioral changes following the Facebook scandal
Facebook scandal	expressions/words/phrases/ non-verbal cues (Fw1)	Facial expressions, phrases, words, and nonverbal cues students make linked to mobile privacy user attitude
Facebook scandal	convenience / laziness (Fw1)	Convenience or laziness trumps mobile privacy user concerns
Facebook scandal	facts	What participants know about the Facebook scandal
GDPR	expressions/words/phrases/ non-verbal cues (Fw1)	Facial expressions, phrases, words, and nonverbal cues students make linked to mobile-privacy user attitude
protection of mobile privacy	expressions/words/ phrases/ non-verbal cues (Fw1)	Facial expressions, phrases, words, and nonverbal cues students make linked to mobile privacy user attitude
protection of mobile privacy	complacency/ learned helplessness (Fw1)	Participants believe they cannot change the situation and/or accept the current situation
protection of mobile privacy	Google/Facebook/ Amazon/Apple (Fw1)	Participants' mentions of any of these companies
protection of mobile privacy	law/regulation/control (Fw1)	Students' thoughts on law, regulations, and control
Facebook scandal	early	Participants think education on privacy, including mobile privacy, should begin at an early age

Table 12 Phase 4: inductive subcategories within main categories with reused subthemes from mobile privacy attitude marked Fieldwork 1 (Fw1)

6.3.3.5 Phase 6: Second Coding Process

All inductive categories were coded. The following table (Table 13) shows the coding framework, including the number of applied codes for the entire data set at the end of Phase 6:

mobile privacy attitude		25
protection of mobile privacy		6
expressions/words/phrases/ non-verbal cues	(Fw1)	4
law regulation control	(Fw1)	9
complacency/learned helplessness	(Fw1)	2
Google, Facebook, Amazon, Apple	(Fw1)	4
mobile security		9
Facebook scandal		25
facts		8
complacency/learned helplessness	(Fw1)	9
convenience laziness	(Fw1)	7
expressions/words/phrases/non-verbal cues	(Fw1)	17
mobile privacy behavior/no_change_yes_change		13
GDPR		15
expressions/words/phrases/non-verbal cues(Fw1)		6
privacy policy update		5
read privacy policy		7
education privacy		13
early		9

Table 13 Phase 6: final coding framework with number of applied codes (right column) and main categories (in bold)

6.3.3.6 Phase 7: Analysis by Summary Grids and Summary Tables

During Phase 7, the coded categories were annotated via the MAXQDA summary grid feature. Then summary tables for each theme were created. All summary tables were exported into MS Word Excel and then printed and carefully reviewed. As a final step, the decision to convert the analysis into a narrative finding via four thematic topics was made.

6.4 Summary

In this chapter, the data-analysis procedure has been summarized.

7. Findings Fieldwork 1

7.1 Overview

This chapter is a narrative formed by interpreting a thick description of the data. The chapter is structured according to topics that deductively and inductively arose from the data analysis.

The first part describes two participants. They are composite characters, "fictionalized individuals whose characteristics are grounded in your research, who represent a typical case, or group of people" (Gullion 2016, 83). Composites are being used in order to better gather and engage with the evidence: according to Jarzabkowski, Bednarek, and Lê, "composite narratives are particularly evidential because, in drawing upon the full breadth of ethnographic data collected and assembling them more efficiently into an evocative story of the underlying patterns identified, they provide greater conceptual generalizability" (2014, 281). The objective is to preview via these two composite characters some of the themes (such as mobile privacy attitude, mobile phone behavior, mobile phone attitude) that are discussed in the findings-by-theme section.

The second part begins with an investigation of participants' mobile phone behavior and mobile phone attitudes. This is followed by a succinct description of the overarching theme of privacy and mobile privacy. Next two major themes: mobile privacy behavior and mobile privacy attitude, including subchapters on location service attitude, privacy policy attitude, and WhatsApp behavior are portrayed. Then a brief addendum on mobile security, which was not part of the original research question but emerged as part of the data analysis is included. The chapter ends with highlighting linguistic expressions.

7.2 Findings: Composite Narrative

The two composite narratives that follow have been created with the same aim discussed by Jarzabkowski, Bednarek, and Lê: "to reveal some typical patterns or dynamics found across multiple observations through one particularly vivid, unified tale." (Jarzabkowski, Bednarek, and Lê 2014, 281).

The first composite narrative is "A Day in the Life of John," which tracks a US Masters of Information student who is based on data derived from seven different student interviews, namely AS1, AS2, AS3, AS4, AS5, AS7, and AS10. There are three reasons why the author of this study, as the ethnographic researcher, feels confident in portraying a real-life narrative of a Rutgers student:

1. She attended SCI&I and obtained her Masters in Communication and Information studies there. Therefore, she has firsthand experience of the classes', students', and professors' interactions and activities. Even though she did not live in student housing, some of her fellow graduate students whom she befriended lived in dormitories. Hence, she is familiar with dorm and graduate student life in the US.
2. As part of her research, she spent many hours on the College Avenue campus and at SC&I to carry out covert observations of students' phone behavior.
3. In her previous career as an academic librarian/assistant professor (see also chapter 1.2 Personal Background), she taught information literacy classes for many years and developed and taught mobile information literacy classes. Her publishing record also focused on mobile learning, mobile information literacy, and mobile technologies concerning academic libraries and libraries at large. As a result, she has been involved thoroughly in both smartphones and higher education for over nine years.

Next the author contrasts the John narrative with "A Day in the Life of Lena," a German Master of Library and Information Science student at Berlin School of Library and Information Science, Humboldt University Berlin *(Humboldt Universität zu Berlin)*. Lena is a composite character assembled from data obtained in interviews with GS1, GS2, GS5, GS7, GS9, and GS10.
While not having obtained a Master's in Germany, the researcher feels confident in portraying a suitable portray because

1. She earned a bachelor's degree in Germany and was a student for four years in Germany;
2. She closely observed both bachelor's and master's students during her time in Berlin at the Berlin School of Library and Information Science, Humboldt University Berlin *(Humboldt Universität zu Berlin)*; and
3. She observed several classes both from the master's and bachelor's programs during her research time in Berlin.

While the activities for both composite characters are fictional, the overarching themes are grounded in collected and analyzed data (see chapter 4 Research Method, and chapter 5 Data Analysis Fieldwork 1).

Themes included in each composite character study are the following:

mobile phone habits and attitudes;
lending of one's smartphone to family/friend;
lending of a smartphone to a stranger;
and mobile security.

Mobile privacy user behavior and *attitudes* are exemplified by *location service behavior* and how the composite characters download the *Perfect Piano app* or what they know and how they interact with their *favorite app*.

Privacy attitudes are briefly addressed by including the themes of *privacy* and *data protection*.

The objective of these composite narratives is to highlight how all these themes matter in relation to the broader context of the dissertation: mobile privacy. They will also help to answer the underlining research question. All composite character quotes are taken verbatim from actual interviews.

7.2.1 American Student: John

The spring semester 2017 at Rutgers University is in full swing. It is the beginning of March, and students all over campus are getting ready for spring break, which is only one week away. At Rutgers's New Brunswick campus, where the SC&I is located, a few trees are already beginning to blossom — a sign that New Jersey's harsh northeastern winter may finally be lifting.

John, 23 years old and with a Bachelor of Arts in Information Technology and Informatics, graduated in the spring of 2016 but decided to continue his education by enrolling in Rutgers's Master's program. He is currently a full-time student taking four classes, with an area of concentration in library and information science. John owns an Apple iPhone 6s.

Beep, beep, beep. John hears his iPhone alarm clock faintly going off. He is tempted to hit the snooze button: it is a cold and gray Wednesday morning, and he doesn't feel like getting out of bed yet. *Beep, beep, beep* – the alarm goes off again. He goes to his iMessages app and sees that some of his friends, as well as his mother, texted the previous night. John quickly replies to his mother; she gets anxious if he does not message her back on time. He decides to text his friends back after he gets some coffee into his body. John quickly goes to Instagram and scrolls through it for a few minutes, then goes to Twitter and does the same. After a quick shower, he gets dressed and checks the time – it is later than he thought. John quickly grabs his backpack and bolts out the door. He puts on his headphones and hits the play button on Spotify: he has "the premium subscription."

As he says, "I walk around a lot and I always listen to music. Let's just say, [if] I am alone, I am always on Spotify." John lives in a dorm on Rutgers's Livingston campus, but all his classes are at the College Avenue campus. While John waits for the bus, he scrolls through Facebook. He also checks out some new messages on the Facebook Messenger app and then goes to Snapchat and start chatting with a friend. "[Snapchat] is entertaining; […] it's like having a text messaging app on your Snapchat, so you [can] message people, you [can] send pictures, […] Instagram does that too, but I like Snapchat better." The bus finally arrives, and during his commute to the College Avenue campus, he opens the Apple mail app. He skims through his personal and school emails: "I check my email really regularly; I don't have more than a handful of emails in my inbox at any one time." John gets off in front of the College Avenue

student center; his stomach is growling and he could really use a coffee. Since John still has a bit of time before his first class, he decides to go to the student center cafeteria. Suddenly a girl, maybe 18 or 19, approaches him and asks if he can help her find her way to the train station. She says that her phone battery just died and she forgot to bring her charger. John ponders — "… my phone has fingerprint security and stuff, and I have things set up so that I can manually wipe it if I need to; iPhones are kind of harder to steal, because you can track them …" — but then he decides to help her. He opens up his phone via his thumbprint. He quickly goes to Google Maps and types in the train station.

Google Maps is one of the apps for which he enables location services. "I don't mind having [location services turned] on, but [there are] some apps I don't like so … my general thing or sometimes never, I don't really want the app to have my information, like Rutgers app I have [location on] while using, Safari I always have, it is just annoying to keep clicking, yes you can use my location, things like Uber, most things are while using it is okay." John's attitude regarding location services has changed over the years. Now, "it is at the back of my head: do you want people to, because I know it says the app, for app purpose, but being in IT classes you always hear how people can always be watching you, something like that, so the past year, I have been kind of eerie about what apps have my location or information like that." John shows the girl the directions on his phone but keeps it in his hands. "I just don't feel comfortable giving someone my phone, [especially] if I don't know them or if I have never met them, or anything, because I see it happen all the time: my friends [have] gotten their phones stolen." John is relieved the girl hasn't asked him to make a phone call, because he is not sure if he would hand her his phone. "[For a] phone call I probably would … keep a keen eye on him or her. It depends again on the situation; I don't know, [it's an] in-the-moment kind of thing … But if they were very desperate … and they just needed to call somebody, I would totally give them my phone." Interestingly, John's mother had recently asked to use his iPhone. She couldn't find her own and needed to call his father. It made John remember the one time his girlfriend wanted to use his phone — which he won't allow. I said, "no, because it is personal … the phone knows more about me than my girlfriend or anybody else." It is "because [of] how close I am with my phone, because I am always on it, there is so much information on it. I don't know what is on it either, there is so much on it, I don't know, because I have pictures, I don't know." I feel like a phone is something — well, it is definitely

something very personal. With the phone you can probably do, so much: it is connected to your bank account, [contains] whatever data that you have, it is connected to your social profiles, it is everything." Going back to John's mother, ultimately, he allowed her to call his father, but "I don't want her to go onto social media on my phone, because I don't know if she is looking through my stuff or sometimes you forgot to log out and their account will be on my phone and I feel really uncomfortable when that happens."

John finally makes it to the cafeteria and gets himself a bagel and latte. Having helped the girl find her way to the train station, he opens Spotify again. As the coffee enters John's system, and he starts to feel more alert. While walking to class, he scrolls through Instagram and direct messages (DMs) two of his friends. He also answers some of his iMessage texts from the previous night. John has two classes today. The first, the one he arrives at now, is called Human Information Behavior. John thinks that the class is all right, the professor is cool, and has fun, engaging discussions. The class covers "diverse contexts of information behavior; processes of information seeking, searching, using, and valuing. Assessment of studies of human information behavior in terms of relevance to library and information services."[20] John prepares for the class by turning off Spotify and putting his phone on "do not disturb" mode. "I try not to use it during class, but if it is there, it is there … I try to concentrate on whatever."

After class, John disables "do not disturb mode "on his iPhone and notices that his mother has tried to reach him. John does not make or receive many phone calls anymore: "mostly I text people or message them because if the [question] can be answered in a sentence or two than there is not exactly much more point to call in the first place." His parents are an exception, and he still talks to them regularly on the phone. John quickly calls his mother back and talks to her while walking to the library. During his phone call with his mother, John checks Twitter, Facebook, Facebook Messenger, Instagram, and his iMessages. John's mother has just gotten her first Apple iPhone; she used to have an Android phone but finally made the switch. Now she always calls John if she cannot figure something out or needs help. John does not mind, and he is happy that she finally has an iPhone, too: "I always had the iPhone. I never wanted to get an Android, I don't like that … I love [the iPhone]. Yeah, I love it, it is very user-friendly."

[20] HUMAN INFORMATION BEHAVIOR | Courses | School of Communication and Information | Rutgers University 2019

It never occurred to John to switch to an Android, "Androids are just terrible [to] use, it is not user-friendly, and also, I have Mac, so, therefore, it connects my text messages to my computer. It is just so much [more convenient] to have this connection between both systems." Last year, John traveled to Italy for the first time, where he noticed that " most people don't even have iPhones. Many people have Androids, and I think if they have iPhones they have iPhones 4s, 5s. It was really interesting to see how everyone in America always wants the new thing, and everyone always has the new thing, but there it is different everywhere you go."

John finally reaches the library. He sits down at a table and unpacks his MacBook. John is glad he found an empty spot in the quiet section as he begins work on a class assignment. While he waits for his Mac to start up, he checks his iPhone for his emails, scrolls through Twitter, and iMessages with his girlfriend.

Then he remembers one of the discussions he just had in his previous class on phone usage versus computer usage. There he'd said, "I use my phone more [often than my laptop] because it is more portable … I just use [my laptop] for school." Even when he has a paper to write or an assignment to complete, he believes that "I am always on [my phone], it is always near me, I feel, you feel the need to have your phone on you all time [and] when it is not with you are a little insecure like you don't know." One of his classmates said, "I mean I use the computer for work and for homework, I mean I use it a lot, [but] it is more of an effort to turn it on, or to lug [it] around, so I probably use the phone more (...) maybe 60/40 percent, 60 percent phone." Also, yet another classmate agreed, adding, "Probably 90 [percent for phone] to 10 [percent for laptop]; 10 percent is only for schoolwork really, and I do everything on my phone really."

Of course, if John has some serious work to do like right now or "maybe on the weekend [iPhone usage] will lessen, because I will be hanging out with friends and I probably wouldn't look at the phone that much, so like I just like living in the present and not bothering about my phone as much." John checks the time on his iPhone and realizes that he should stop procrastinating. He sets the timer on his phone for two hours and then dives into his assigned readings.

After two hours, John's brain hurts, and he decides to get another coffee. He needs to be alert for his next class, Information Policy, which is about the "economic, social, and political forces affecting the introduction and implementation of current information legislation and policy, set within the theoretical context of frame reflection"[21] John likes this class to some degree as well, but finds the required readings just *too much*. He walks to Starbucks, again listening to Spotify. While John waits for his Grande Latte, he scrolls through his Twitter and Instagram feeds, checks his email, and reads through a message on GroupMe, which his Information Policy class uses. One of his fellow grad students was confused about the dates for spring break and thought there would not be a class this afternoon. John quickly messages that they *do* have class and hopes to see him in a bit. John walks back to SC&I, finds his classroom, and puts his iPhone into "do not disturb" mode. John is not in the mood for this class right now and cannot wait for spring break to start.

It turns out the class is enjoyable, and the 90 minutes go by very quickly. The professor divided the class into different groups, and each group had to brainstorm what privacy and data protection means for them as a digital citizen. John's group got into a heated discussion on whether privacy is even possible nowadays, on what things they consider private, and how the perception of privacy is different from just twenty or even ten years ago, before the iPhone changed the mobile-phone world forever.

John said that "privacy is selecting what you want others to see, whether be it a friend or foe or just people or everyone, [giving them] that access to the app, website. It is what you want to show people and what you want to keep to yourself." But he also said "I feel like that definition would have changed as time goes by … Privacy is kind of dated anyway; even if data is anonymized you can probably identify that person based on specific [information] that you have — you just look and analyze the postal code, and you can basically filter down … and find that person. That's why it is actually pretty easy to me [to say] privacy is actually dead, but if you ask me what privacy is, it is probably, [keeping] the information to yourself."

His group found it very challenging to come up with a definition for data protection. John chimed in with, "data protection, that is usually like software or stuff that a website promises

[21] INFORMATION POLICY| Courses | School of Communication and Information | Rutgers University2019

you, where they personally make sure that your data doesn't get out anywhere, without your permission and no harmful elements can get/have access to your information." It was stimulating to think about these two terms – privacy and data protection. The professor wants the class groups to go online and find two scholarly articles for each topic. Then as a group, they have to do a short presentation on it. John's team just set up a GroupMe group, and they agreed to do some work over spring break. Fortunately, this presentation is not due until three weeks after break, so John does not feel too stressed about it yet.

As John makes his way to the bus stop, he again listens to Spotify. He also checks "the Rutgers app; they have an app for the bus schedule, so I can look when the bus is coming." While he waits for the bus, he scrolls through Snapchat, Instagram, and Twitter, and iMessages with his girlfriend and mother. The bus arrives, and he gets off in front of the gym. John has not exercised at all this week, and he feels it might help him to relax and unwind before finishing his paper for the Human Behavior class. It is due this Friday, and although he already started, he would like to get some more writing done tonight. John changes into his gym clothes and decides to do a 30-minute workout on the StairMaster. He puts his iPhone in front of him and goes to YouTube. John likes watching YouTube during his workouts "because I like seeing all those videos; there is a bunch of original content or remixed content that I find funny or interesting, it is just like you can find anything on there." After his workout, he hits the shower, gets changed, and walks home to his dorm. Of course, he listens to Spotify during his quick walk back.

John finally gets back to his dorm room, unpacks his MacBook, and turns it on. He really needs to work on his assignment, but decides to eat first. While he waits for leftover pizza to reheat in the microwave, he scrolls through his iPhone, going to his Facebook feed and skimming through some stuff. Some of his friends "say [they would] get rid of Facebook if it wasn't for Messenger," but John thinks "I also get a feel [for] what is kind of trending, what is going on in the world … I get a lot of news from Facebook, I like sharing things, I have a lot of interests, and I get to keep in touch with, like, family, which is a big thing for my friends and me." John stays on Facebook for about 30 minutes, well, maybe longer.

John manages to work on his paper for about two hours. It is still not completed, but he feels it is in pretty good shape. He only has one class tomorrow and none on Friday, so that leaves

him with enough time to get it done. John has not checked his phone in approximately 30 minutes. John picks it up and sees that he has gotten a few new DMs on Instagram and an iMessage from his mother's friend, Olivia. Olivia is this cool old lady, she is maybe in her eighties already, but she is still woke. She lives in New York City and is totally into all Apple things. She owns an iPad and an iPhone and has told John that her next computer will be a MacBook, because that is what she sees all "the kids" (her words, not his) using at Starbucks. She wants John to help her install an app on her iPhone. John guesses she has not done it for a while and forgotten how. He calls and walks her through the process of downloading and installing the Perfect Piano app. Since John is not familiar with this particular app he says, "When I download an app, I go to the stars to see reviews, [and] if it looks interesting, try it out." He tells her how to download it and then does the same. "I just click 'get,' and then it is done, use my fingerprint and that's it." After it is installed, he tells Olivia to open up the app, and he does the same.

"It would like to send me notifications; I don't like notifications, to be honest." He tells Olivia to click on "don't allow," because notifications "are just disruptions I guess, actually it depends on the app, so if it is an app, that I am going to be frequently using then I probably put allow, but if it is not, then I just don't allow." Olivia manages to follow John's instructions, and then they talk for a few more minutes. She tells him how she did not even have a landline growing up, much less a TV, and of course no internet at all.

John vaguely remembers when he got his first smartphone: "It was pretty cool, because going from a flip phone to touchscreen and all the apps, it was cool, I enjoyed it." He then says goodnight to Olivia and tells her to enjoy playing around with her new app. John checks the time on his phone and realizes that it is getting late. He changes into his pajamas and brushes his teeth. He lays down on his bed and scrolls through Instagram, Facebook, Twitter, and Snapchat. Simultaneously, he iMessages with his girlfriend and a few of his friends. One hour later, he finally decides to go to sleep. John makes sure his alarm is set for the next morning and puts his phone next to him on his nightstand before drifting off into sleep.

7.2.2 German Student: Lena

Lena is a 26-year-old master's student originally from Stuttgart, Germany. She holds a Bachelor of Arts in Information Science from the Hochschule der Medien, Stuttgart. Lena finished her bachelor's degree two and a half years ago and worked as a web developer at a web design agency in Munich. During her time there, she befriended an academic librarian and realized that in the long run she would be more interested in a similar career. Therefore, she decided to enroll in the Master of Library and Information Science program in Berlin. She is currently in her fourth and final semester and is writing her master's thesis. Aside from being a full-time student, Lena works 15 hours a week at a web design agency in Berlin. She lives with two roommates in an apartment in Neukölln (a district of Berlin). Lena currently owns a Samsung Galaxy S5.

It is mid-January 2017, and Berlin is still in the midst of winter. It is a damp and cold Monday morning when the alarm in Lena's room goes off. *Beep, beep, beep.* Lena hits the snooze button on her phone. "Well, of course, I also use it as my alarm clock." *("Ach so, ich benütze es auch als Wecker natürlich.")* She is not yet ready to face the day and needs ten more minutes in bed. *Beep, beep, beep,* Lena's alarm clock is going off again. Lena takes her phone into her hand and turns the alarm off. Then she opens an app to read her email. "I noticed how quickly I developed a habit, for example, in the morning — I mean, the phone is my alarm clock, so the first thing I do is take my phone in my hands, and then I check my email, look for something online and the news. I am considering buying myself an old-fashioned alarm clock again, so that I don't use the phone and get annoyed because I read an email from the tax department first thing in the morning." *("Ich habe gemerkt, dass sich ganz schnell so Gewohnheiten einschleichen, so am Morgen, so der Handy Wecker funktioniert natürlich auch über das Smartphone und dass erstmal das Handy in der Hand und dann schaue ich erstmal meine E-Mail an und dann schaue ich noch irgendwie Internet noch die Nachrichten an und so und habe mir jetzt tatsächlich überlegt, ob ich mir nicht einen Radiowecker kaufen soll, um den entgegenzuwirken, um eben nicht nach dem Aufwachen so die nervige E-Mail vom Finanzamt zu lesen.")*

After Lena uses her phone to procrastinate for a short time, she gets out of bed and walks to the bathroom. It is still a bit too cold for her taste, and she takes a hot shower to wake up

fully. After the shower, Lena goes into the kitchen and begins making herself coffee. While she waits for the coffee to be ready, she looks at the Wunderlist app on her phone to see what chores and to-dos she has scheduled for today. "I can't live without [Wunderlist] anymore. I have everything in it, from small things to long-term projects, stuff like cleaning the apartment and inviting my parents … stuff like that is in it too." *("Ohne die [Wunderlist] komme ich gar nicht mehr klar, ich habe da halt alles drin, also alle Sachen von kleinen Aufgaben, aber auch längerfristige Projekte, die man so macht, so was wie Wohnung putzen und Eltern einladen und so, das ist da auch alles drinnen.")* Finally, the coffee is ready and Lena sits down with her muesli and eats breakfast. According to Wunderlist, her tasks for today include going to the library and working on her master's thesis for a few hours, meeting a friend at the cafeteria *(Mensa)* for lunch. After lunch, she has to go to work for three to four hours. Later in the evening, she has choir practice with the Philharmonischen Chor Berlin. Usually, after the practice, some people go to a local pub nearby for a few drinks, but Lena is not sure yet if she will go tonight. She feels a bit stressed, because she has a lot of work still to do for her thesis. Lena scrolls through Facebook for a few minutes and then checks Facebook Messenger and WhatsApp for new messages. She quickly writes her sister back. She needs to get her sister to purchase Threema, a secure messaging app. "I only use WhatsApp because some people don't have Threema." *("Ja ich benütze eigentlich WhatsApp, nur weil manche Leute kein Threema haben.")* It is not easy to convince people to use Threema: it is "a long process; Threema costs like two euros, it is sort of a mission: 'Come on, pay two euros.'" *("Die, also es war ein langer Prozess so – ... Threema kostet auch so zwei Euro, das war schon immer so ein Akt, zahl doch mal die zwei Euro.")*

Before Lena gets ready to head out the door, she checks the BVG app for subway times and a weather app for the forecast. It seems it is going to be a sunnier day, and so she might get off a few stops earlier and walk through the Brandenburg Gate on her way to the university library. Lena likes to walk at times, as it helps her to clear her mind. "To kill time while commuting in the subway, I play a game called Atomas." *("Ja während der U-Bahn-Fahrt, um die Zeit zu überbrücken, spiele ich so ein kleines Spiel, Atomas heißt das.")* She remembers how "the day before yesterday, my phone turned itself off without warning. In the middle of the day, and for the rest of the day, I couldn't use my phone anymore. That was so annoying — I mean it was like, I couldn't do anything at all." *("… vorgestern ist mein Handy überraschend*

ausgegangen mitten am Tag und dann hatte ich den halben Tag mein Handy nicht mehr und das war schon das war super nervig, ich konnte gar nichts mehr machen.") Lena doesn't consider herself an early tech adopter; she purchased her first smartphone in 2013. However, she has to admit that "one gets used to it so quickly. It is like always being connected, it changes, and I, um, I don't know, I mean to be addicted sounds a bit too strong, I mean, I don't think I am addicted to my phone, but maybe if anything, to the services one can use with it … it always depends how I feel, and how much I want to procrastinate." *("Man gewöhnt sich halt sauschnell daran, ist schon so, also die Erreichbarkeit, ähm wird anders und ich äh und ich weiß auch, also abhängig ist vielleicht bisschen übertrieben, ich glaube ich bin nicht vom Gerät abhängig, sondern wenn dann von den Systemen, die man damit bedienen kann, ... da kommt es immer auf Phasen darauf an, wieviel ich prokrastinieren will.")*

Lena gets out of the subway and starts walking toward the Brandenburg Gate. She decides to take the phone out of her pocket. She wants to turn on location services and use it for Google maps. She has to trace her fingers in a complicated pattern to open the screen lock: having to do that " can be annoying. For example, if I want to take a photo, and the sun is glaring, then it takes me forever to enter my code, forever before I can take the photo. I set it up because I lost my phone once. I mean, luckily nothing happened, I just returned to the place and it was still there, but the simpler lock patterns, those are so simple, I mean the fingerprints on the screen kind of let you trace the pattern." *("... habe ich hier so einen recht komplizierten Code, was auch richtig nervig ist. Wenn man zum Beispiel ein Foto machen will und dann spiegelt die Sonne so ein bisschen und dann gibt man erstmal so zehn Tage lang seinen Code ein, bis man ein Foto machen kann. Das habe ich auch mal eingerichtet. Und als ich es mal kurz verloren hatte, ist gar nichts passiert, ich bin einfach wieder an den Ort zurück gegangen und habe es wiedergefunden. Bei diesen Wisch Codes zieht man ja total oft voll einfach an den Spuren auf dem Display, wie der Code war ...")*

After Lena unlocks her phone, she enables location services for Google Maps as "I usually have it turned off [clicks on Bluetooth and location services], I have it off, and Bluetooth, too." *("das, das habe ich eigentlich immer, das habe ich hier oben da Standorte [geht auf Bluetooth und Standorte] das habe ich eigentlich immer aus, Bluetooth und das.")*

Lena looks at Google Maps to orient herself and decides to use it as a guide, before turning it off as soon as she becomes more familiar with her surroundings. She does not want to be trackable, since "Google wants to know where I am all the time … which sorta sucks." *("Google ja sonst ununterbrochen weiß wo ich bin … Ne also des ist gar kein Hit.")*

Lena starts walking and is still taken aback at the sight of the Brandenburg Gate, even after living in Berlin for quite some time now. As usual, there are many tourists. Suddenly, a man approaches and asks her if she would mind taking a photo of him and his wife in front of the gate. Lena is happy to help, and he hands her his iPhone 7. This is something Lena is still puzzled by: "I am sometimes surprised how often I am asked by someone in Berlin to take a photo. I am a bit puzzled, and think, what if that were MY [emphasized] iPhone, would it be giving it to you?" *("ich bin ja manchmal schon etwas verwundert, wie oft man in Berlin gefragt wird, ob man mal ein Foto machen würde von jemand anderen mit dem Handy und wo ich mir auch manchmal kurz denke, wenn ICH [Betonung auf ich] der jetzt wäre, du gibst mir jetzt dein iPhone in die Hand.")*

Lena wonders what the man would do if she were to run away with his expensive iPhone, since to her handing her phone to a stranger would be "really stupid. Not only because of the value of my phone, but also because of all the information on it." *("das ist auf jeden Fall doof jetzt, wenn es jetzt weg ist, von daher wegen dem Geld und dann halt auch wegen den ganzen Informationen, die da drauf sind.")* She wouldn't even give her parents her phone even though, she admits, "I should trust them. But, nevertheless, I do all sorts of things on my phone. If someone has my phone, they have access to everything, like who I talk to, what I talk about, what I am doing." *("man sollte eigentlich Vertrauen haben, aber trotzdem auf dem Handy mache ich ja alles Mögliche, wenn man mein Handy hat, dann hat man eigentlich so Zugriff auf alles, mit wem ich spreche, worüber ich spreche, was ich tue, also es ist, wäre mir schon nicht recht, glaube ich.")*

Of course, she would never run off with someone's phone. She takes a picture with the iPhone 7 and then hands it back to the tourist. Lena used to have an iPod, but she "didn't want an iPhone because of the price tag, and then it is a closed ecosystem, with regard to music and everything else." *("wollte kein iPhone, erstens wegen des Preises natürlich und weil es auch so ein geschlossenes Ökosystem ist, mit Musik und allen.")*

Lena is quite happy with her Android-based Samsung Galaxy S5: "In terms of features, it is only a little less powerful than the S6, but it is way cheaper and that's why the value is really great." *("Es hat halt nur unwesentlich schwächere Funktionen als das S6, aber ist halt preislich viel günstiger und deswegen ist das Preis-Leistungs-Verhältnis unglaublich gut.")*

Lena continues her walk, and as she is now more familiar with the neighborhood, she turns location services off, closes Google Maps, and tucks her phone into her bag. After another twenty minutes, Lena finally reaches the university library. She goes in, finds a quiet spot, sits down at the table, and unpacks her laptop. Then she remembers an interesting phone conversation she had the other day with her father. He doesn't own a smartphone — "well, my dad wouldn't know what to do with it [she is laughing]; my mom owns one now, but my dad doesn't." *("gut mein Papa wüsste wahrscheinlich gar nicht, was er damit machen soll, [sie lacht], meine Mama hat mittlerweile auch eins, aber mein Vater gar nicht. ")*
In any case, her father had asked her if she uses her phone more than her computer these days. At first, Lena thought it a strange question to ask, as the answer is, of course, her laptop, but then she had to admit, "to be honest, it's 60% phone and 40% laptop. On my laptop I do things that are more complicated and take me longer, and that's why I spend more time on my laptop, even if I'm not on it as often." *("Also wirklich 60 Prozent Handy und 40 Prozent Laptop, weil auf dem Laptop mach ich ja Sachen, die die länger dauern oder aufwendiger sind, deswegen verbringe ich da längere Zeit, aber nicht so häufig.")*
However, then she told her father that right now, while she is working intensely on her thesis, it might be "70% of the day in front of the PC and 30% on the phone, but perhaps on the weekend it is different again, and I'll use the phone more." *("70% Prozent des Tages bestimmt vor dem Rechner und 30% am Handy, aber, wenn es am Wochenende ist, ist es wieder ein bisschen anders, da bin ich vielleicht mehr am Handy.")*

Lena's laptop is ready, but she not quite in the mood to start writing. She unpacks her phone and looks at WhatsApp, writes a message to her boyfriend on Threema, and then checks Facebook Messenger and Facebook. "I thought about removing Facebook from my phone, because sometimes I waste time on it while waiting for the subway. I scroll around Facebook – it is a time suck – but on the computer, I would like to keep it … because I have a lot of old friends who are also on Facebook, and that's how I keep in touch. I know a bit of what they

are up to, and I kind of like that." *("Ich habe mir, ich hab mir schon überlegt, ob ich Facebook von meinen Handy entferne, weil ich auch oft sinnlos dann an der Haltestelle stehe und bisschen auf Facebook rumscrolle so, was man sich eigentlich auch sparen könnte, aber auf dem Computer habe ich es auf jeden Fall, weil ... ja, hab halt, viele Freunde auch von früher und so, die auch auf Facebook sind, und so hat man noch bisschen Kontakt und kriegt ein bisschen mit, was die anderen so machen, und das finde ich eigentlich auch ganz schön.")*
Lena checks her phone for the time — it is already 10:30 am and she is supposed to meet her friend at 1 pm for lunch at the university cafeteria. Lena puts the phone next to her laptop, turns on silent mode, and starts to write.

After an hour "my writing isn't flowing anymore, and I look at my phone; maybe something has happened, something distracts me, it is like being on autopilot, totally automated. Most of the time nothing has happened and then I continue to work." *("und dann läuft es mal nicht so und dann schaue ich auf das Handy, vielleicht ist ja was passiert, was mich ablenken könnte. Und das ist echt so ein Mechanismus, das ist total automatisch. Und meisten ist gar nichts passiert und dann schreibe ich auch weiter.")* Lena spends a few more minutes messaging with her boyfriend on Threema and also checking out the Bored Panda app, but then she sighs and goes back to working on her thesis.

Around 12:45 pm, she closes her thesis documents and quickly messages her friend via Facebook Messenger that she is on her way to the university cafeteria. While she walks toward the cafeteria her phone rings, which is "really, totally strange." *("Also wirklich, das ist ganz krass, wenn es mal klingelt.")* Lena does not recognize the number and ignores the call. She can see her friend Brigitte waiting in front of the cafeteria and starts to walk a bit faster. After saying hello to each other, they walk into the cafeteria and started queuing for food. Lena originally met Brigitte through Lena's boyfriend; Brigitte and Lena hit it off and now often eat lunch together in the cafeteria. Brigitte is studying law and wants to become a defense lawyer. After both women pay for their food, they find a table and start eating and talking. Brigitte just attended a seminar on data protection and wants to know what data protection means to Lena.

At first, Lena is a bit puzzled; she hadn't thought about data protection in a while, but then she answers, "oh, well, data protection is, to me, having the guarantee that my

data/information is encrypted and so nobody else can get to it. Let's say my Facebook account is hacked, so nobody would see where I live, what my phone number is — that's data protection for me, sort of how I can deposit my information/personal data for certain things … but I can assume that they are then secure and that not everyone has access to it." *("Ja Datenschutz ist eigentlich für mich das, was mir gewähren soll, dass meine Daten so verschlüsselt sind, dass die niemand anders an die rankommt, also dass jetzt nicht jemand, wenn der meinen Facebook account hacked [sic] zum Beispiel, dass der sieht, wo ich wohne, meine Telefonnummer. Also das ist eigentlich für mich Datenschutz, dass ich zwar meine Daten irgendwo hinterlegen kann für gewisse Sachen, … davon ausgehen kann oder sicher sein kann, dass die [Daten] da sicher sind da, geschützt sind, dass da nicht jeder Zugriff hat.")* Brigitte is impressed with Lena's answer and says with a chuckle that perhaps she should switch to law studies. Lena shakes her head but continues: "and to go back to data protection, well, one has to actively take part in protecting one's personal information and data. Everyone wants your info these days, so you have to protect it." *("Und dann auf Datenschutz zurückzukommen, dass ist, was worum man sich auf jeden Fall kümmern muss und wo man aufpassen muss, weil jeder will halt die Daten, die muss man auf jeden Fall aktiv schützen.")*

Brigitte looks at her phone and realizes that it is getting late. Lena also has to get going, since she has to work. After lunch, both women say goodbye and head in different directions. Lena takes the subway, again playing Atomas during her commute, but also checking her work email. After a few stops, she arrives at the subway station and walks to her part-time job as a web developer. The small web agency's office is rather quiet today; everyone seems to be fully immersed in their Macs or PCs. Lena says hello to all her coworkers and then turns her PC on. While she waits for it to start up, she scrolls through her emails and Facebook Messenger. She has new messages from a friend and her sister, and one new one on Threema from her boyfriend. Since she is at work, she puts her phone back into her bag and starts concentrating on her tasks.

After about two hours of concentrated work, Lena gets up, unpacks her phone, and goes into the kitchen to make herself a coffee. While standing in the kitchen and drinking her coffee, she checks her email, goes through Facebook, and texts via Threema with her boyfriend, Torsten. "Yes, I look at my phone a lot. According to my boyfriend, I should look at it less. I sorta constantly feel the need to check my emails." *("Ja, ich gucke schon viel auf das Handy,*

mein Freund sagt auch, ich sollte es mal ein bisschen reduzieren, ich habe manchmal den Drang ständig meine Mails zu checken, einfach so.")

Lena is about to head back to her desk when one of her coworkers enters the kitchen. She wants to know more about the app Lena uses to schedule her projects and tasks. Lena tells her about Wunderlist and how much she uses and relies on it. Her coworker asks about Wunderlist's security and privacy protection. Lena has to admit, "I don't know. I mean, I looked at it when I first downloaded the app, but then I forgot about it, ahem, with Wunderlist, in terms of data protection/privacy, I mean well, I guess, I have my entire life in it, and I know that, and I guess, I don't know how much they evaluate it statistically, semantic evaluation or stuff like that. I mean I don't know that." *("Das weiß ich nämlich nicht, sowas gucke ich am Anfang nach und dann vergesse ich es sofort wieder, ähm gerade bei Wunderlich ist es Datenschutzrecht-technisch, also ich habe ja gesagt, ich habe mein komplettes Leben darin abgebildet und dessen bin ich mir auch bewusst, wenn sich da, ich weiß nicht in wieweit die eine Auswertung machen, semantische Aufgaben, Auswertung oder sowas, ahme, ne das weiß ich gar nicht.")*

Another coworker comes into the kitchen, and the three talk a bit about their favorite apps and the best ways to choose a new app. Lena tells them that during the installation process she usually "[glances] at the permissions. If it asks for camera or photo access, I usually wonder if the app really needs it, and do I really need the app. Especially with camera and photos, I am usually a bit more careful since I don't like it when apps can access my photos." *("da gucke ich erstmal immer, wenn es fragt, Kamera-Zugriff, Fotos-Zugriff und dann gucke ich auch, braucht es die App wirklich und wenn ja ist es mir das Wert, vor allem bei Fotos und Kamera bin ich ein bisschen vorsichtig, weil ich es nicht so gut finde, dass jede App auf deine Fotos zugreifen will.")*

After a few more minutes of chitchat Lena and her coworkers all head back to their desks. Lena puts her phone back into her bag and goes back to her work. After another two hours of concentrated coding, Lena is starting to feel tired and a bit hungry. She decided to call it a day and head home for a bit before choir practice. During her subway commute Lena spends most of the time listening to a podcast she listens to via Podcast Addict, she confesses, "well, yes, I use it a lot". *("Podcast Addict ... Genau ja, die benutze ich sehr viel.")* After about 45 minutes

she is back home and has time to reheat leftover soup for dinner. While Lena eats, she turns on her laptop to reread a few pages of her thesis. She still has a lot to do and is glad that tomorrow she will not have to work and can spend the entire day writing in the library.

After half an hour of reading and editing her thesis, Lena checks her phone for messages, emails, and the weather forecast. She also takes a quick look at Wunderlist for her schedule for the rest of the week. During her train ride to choir practice, Lena again listens to a podcast using Podcast Addict. Lena arrives just in time for choir practice, turning her phone off and leaving it in her bag. The choir conductor does not like it at all if anyone looks at their phones during practice – even worse, he usually gets upset if someone's phone rings during practice time.

After one hour of intense practice, the choir gets a 15-minute break. Lena takes her phone out of her bag, turns it on, and scrolls through Facebook for a few minutes, reads a few WhatsApp messages, and texts her boyfriend on Threema. She starts chatting with her fellow soprano choir members and they start talking about the best ways to practice at home. Lena holds up her phone and recommends the free Perfect Piano app. Lena likes using it to "learn to sing some scores, and sometimes, I don't know how the tone is supposed to sound if I sing it alone at home." *("Partituren singen lernen und manchmal weiß ich nicht, wie Töne klingen, wenn ich was alleine singen muss zuhause.")*

Break time is over, and for the next hour, Lena keeps her phone back in her bag and focuses on choir practice. After practice is over, Lena heads home, too tired to go with her fellow choir members to socialize in the local pub. Lena takes her phone out of the bag, turns it on, and quickly scrolls through her emails, WhatsApp, and Threema. She quickly checks the BVG app for the subway schedule. During her commute home, Lena scrolls a bit through Facebook while simultaneously listening to a podcast. Finally, after about 45 minutes, Lena reaches her apartment. She puts on her pajamas, brushes her teeth, and goes to bed. For the next 20 minutes, she messages with her boyfriend via Threema. Tomorrow, they will see each other for dinner. Lena makes sure the alarm clock on her phone is set and then puts her phone on her nightstand. As Lena slowly drifts into sleep, she thinks about all the writing she wants to get done on her thesis tomorrow.

7.3 Findings by Themes

In the following subchapters the results of the interviews are shown by main and subcategories to describe the broader context of mobile privacy.

In every subchapter, first the answers and reactions of German and then of American students are shown. Through this approach analogies and differences in thinking, attitudes, and behavior are more apparent and easier to discern and analyze.

To make the characters more relatable assigned pseudonyms to each of the students, as in the tables below (Table 14 + 15).

GS1	GS2	GS3	GS4	GS5	GS6	GS7	GS8	GS9	GS10
Elke	Heike	Jörg	Berthold	Saskia	Florian	Ute	Wolfgang	Beate	Ralf

Table 14 German participants

AS1	AS2	AS3	AS4	AS5	AS6	AS7	AS8	AS9	AS10
Steve	Jack	Ava	Luke	Abigail	Harper	Liam	Owen	Ryan	Marsha

Table 15 American participants

7.3.1 Mobile Phone Behavior

The following sections detail German and American students' smartphone habits.

7.3.1.1 German Students

While talking to students about their daily phone usage, I was curious to see how students would estimate and calculate it.[22] Generally speaking, most German participants admit to using their phones quite often. Some students note that they use it as their watch (Ute and Saskia) and thus look at it more than they would otherwise. For Saskia, the habit of checking the time became so compulsory that she bought herself a new watch.

[22] This was before both Apple and Android introduced tools to monitor screen time:
https://techcrunch.com/2018/05/08/android-rolls-out-a-suite-of-time-management-controls-to-promote-more-healthy-app-usage
https://www.macworld.com/article/3305557/how-to-use-screen-time-in-ios.html

The five students that I consider late-majority and laggard smartphone adopters (Ralf, Beate, Florian, Jörg, Elke) openly admit to how quickly they became accustomed to their phone, and also exhibit what they consider bad mobile phone habits. For example, Ralf used to hate it when people looked at their phone while he was having a conversation with them, but now admitted his behavior is much the same. Consequently, he hides his phone in his backpack during university time; he does not want to become, or be like, "everyone else."

Jörg, the laggard smartphone adopter, confesses to always being on his phone: it worked itself into his and his girlfriend's lives very quickly.

Heike has to remind herself to not always check her phone. At times she purposely leaves it in another room or turns on silent mode. She notes how people once used to be unavailable at times, and how that was normal.

Elke and Beate both became accustomed to their phone very quickly, but admit that some habits are not necessarily good ones. Elke points out that checking her email first thing in the morning stresses her out, and Beate talks about the phone operating as a procrastination tool. Several other students mention procrastination as one of their principal phone habits. For example, instead of working on a paper or being productive at work, they use their phone to check messages or surf the internet.

Florian deviates from the others in that he thinks using his phone at work is improper. He works in a library, and he considers it inappropriate and bad manners to use it during work hours:

> I store it in my bag so I won't use it. I turn it off. In my opinion, it is not appropriate to use it while I am working.
>
> *Ich packe es weg, in die Tasche, dass ich es nicht mehr berühre, stelle es aus. Weil das hat für meine Augen, auf der Arbeit nichts zu suchen.*

Asked about their perceived difference between weekend and weekday usage, three students (Beate, Florian, and Heike) remark that they use it less on the weekend since they are busy with social activities; Florian points out that his smartphone is not his entertainment device.

Many students had difficulty estimating their phone usage as compared to their computer usage. The overall consensus? Smartphone use is more frequent, but for shorter periods of time, while the computer is used less frequently, but for longer periods of time, and for more serious work, such as studying.

When talking to students about the primary use of their smartphones, they all mention communication via messaging apps (WhatsApp, Signal, Threema, Facebook Messenger), using various navigation tools such as commuter apps and Google maps, using the browser to search for and find information, taking pictures with the camera, and social networking (primarily Facebook).

Several students also use their phones to email, listen to music, as an alarm clock/clock, and to play games.

Two students expressly point out that they do not use email on their phones: Ute because she does not like the usability of the mail apps, and she thinks that communication via the Messenger apps is enough; and Florian because he uses his phone to relax, and checking email would interfere with that.

The German students ranked their top five apps as follows- see Table 16:

Ralf	Podcast Addict	AnkiDroid	**Threema**	Öffi	Here
Beate	**Telegram**	calendar app	Plant Nanny	Headspace	
Wolfgang	**Whatsapp**	**Spotify**	**Facebook Messenger**	Wikipedia	Google Chrome
Ute	Wunderlist	**WhatsApp**	**Signal**	VLC player	BVG app
Florian	*Threema*	Aldilife	VPN	*Google Maps*	My Number
Saskia	**WhatsApp**	**Facebook Messenger**	**Spotify**	BlueMail	BVG app
Berthold	Öffi	Drive Now	Firefox browser	**Signal**	**Google Maps**
Jörg only lists three	**WhatsApp**	**Facebook Messenger**	PDF reader	---	---
Heike	**WhatsApp**	**Facebook**	Skype	Email app (not Gmail though)	Duolingo
					Escosia
Elke only lists four	**Threema**	**Telegram**	DB Navigator	Bored Panda	

Table 16 German students and their five most favorite apps
(bold stands for multiple occurrences among applicants)

So, the most favorite app for them are:

WhatsApp (Heike, Jörg, Saskia, Ute, Wolfgang)

Threema	(Ralf, Elke, Florian)
Facebook Messenger	(Jörg, Saskia, Wolfgang)
Telegram	(Beate, Elke)
Spotify	(Saskia, Wolfgang)
Signal	(Berthold, Ute)
Google Maps	(Florian, Berthold)

Only four students (Elke, Jörg, Heike Saskia) explicitly mention phone calls as one of the main uses of their smartphone – Elke cites it after a long pause, Heike and Jörg laugh, and Saskia finds it bizarre and strange when her phone rings.

7.3.1.2 American Students

Three students commented that they do not use their phone "all the time" (Marsha, Ryan, Owen). Marsha and Ryan, who are both late-majority adopters/laggards, both comment about not using it a lot at work. Owen, an early smartphone adopter, does not use it a lot at work either (he is a substitute teacher), since they told him during a substitute teacher workshop to keep the phone in his pocket. Marsha also declares that if she is spending quality time with her boyfriend and friends, she does not want to be on the phone. She shares this sentiment with Luke and Ava. Ava specifically mentions how rude she finds it if she on a date with someone, and her date is constantly on their phone.

The other participants all admit to using their phone too much, and often because it is their connection to the world. When asked, Steve pauses for a moment and then says, "Shit, like … Oh god … fifty, no, no, no, it is definitely more than fifty. Eighty times a day … that sounds about right." Some students estimated that their usage decreases during the weekend. Owen has a tablet he prefers to use while at home. Harper and Luke participate in more social activities and thus spend less time on their phones. Ava says her usage increases on weekends since she is more socially active, texting more often and spending more time on social media. Comparing their phone usage with their computer usage, six students estimate that they use their phones more. Marsha finds that it is an effort to turn on the computer or to lug the laptop around. Abigail finds it is easier to access her apps and social media on the phone, and Jack also finds his phone to be more portable.

Some students (Owen, Luke, Steve) prefer to use their computer for work that is time-intensive, such as assignments, writing papers, and coding. Harper prefers to use her computer if she needs work on sensitive and or essential documents, such as filing taxes.

Students' phone habits run from

communication via text (iMessage/other text apps, Facebook Messenger),

communication via social media (Twitter, Facebook, Instagram, Snapchat),

music, accessing navigation aid via Google Maps, emailing, reading news via feeds on apps and/or browsers, YouTube, taking photos, playing games, reading (textbooks), and using the clock.

American students rank their five favorite and top apps as follows (see Table 17):

Marsha	**Facebook**	**Instagram**	Whole Foods app	**iMessage**	email app
Ryan	Podcast Addict	**Google Maps**	Google Now	Textra	Google Mail
Owen	Poweramp	**YouTube**	Firefox	Google Hangouts	Reddit
Liam	Twitter	**Instagram**	**YouTube**	**Safari**	**iMessage**
Harper	*Facebook*	**Instagram**	*Snapchat*	GroupMe	text messaging app
Abigail	**Spotify**	**Snapchat**	**Instagram**	**Facebook**	Mail app
Luke	**Spotify**	Facebook messenger	Shazam	**Google maps**	Rutgers app
Ava lists only four apps	IFTTT	**Facebook**	Genius Scan	**iMessage**	---
Jack	music (app)	**iMessage**	**Snapchat**	**Safari**	GroupMe
Steve	Gmail	**YouTube**	**Facebook**	Amazon music	weather channel

Table 17 American students and their five most favorite apps
(bold stands for multiple occurrences among applicants)

So, their most favorite apps are:

Facebook	(Abigail, Ava, Harper, Marsha, Steve)
Instagram	(Abigail, Harper, Liam, Marsha)
YouTube	(Liam, Owen, Steve)
iMessage	(Ava, Jack, Liam, Marsha)
Snapchat	(Abigail, Harper, Jack)
Spotify	(Abigail, Luke)
Google Maps	(Like, Ryan)
Safari	(Jack, Liam)

Only four students mention phone calls at all. Marsha, Ryan, and Ava still make calls, with Marsha stating, "… But I still think, like, it is a phone, and I make phone calls." While Harper apologizes, "Yes, yes, sorry phone calls, I use it for phone calls, it is easier for people I know [who] are actually answering the phone."

7.3.2 Mobile Phone Attitude

Much has been written about smartphone attachment and personification. Before taking an in-depth look at mobile privacy behavior and mobile privacy attitude, it is essential to explain how participants feel about their smartphones in general.

7.3.2.1 German Students

None of the German participants owns an iPhone. Students consider Apple's mobile operating system too restrictive and laden with too much proprietary software. It is a closed ecosystem, says student Elke, and it does not offer much flexibility to be fixed or upgraded.

Beate talks about her frustrating experiences with her iPod. She has owned it for some time, and she still likes it. Unfortunately, she cannot upgrade it to the newest iOS anymore since the hardware is out-of-date. She's afraid that she would have a similar experience if she bought an iPhone. She says that if you know the right people, they can help you fix your Android, but if you have an iPhone, you have to rely on Apple. Heike said she does not need the newest iPhone – all she wants is a phone that functions and works with WhatsApp.

Jörg was the only student with a Windows phone,[23] but during the interview, he mentions he is waiting for his new phone, which is an Android. He prefers Android's usability and the touch keyboard over his current Windows phone. However, he then said that it was more a matter of emotional feeling.
Elke specifically wants her new phone to be able to run on CyanogenMod,[24] an open-source mobile operating system she deems superior to Google's Android system. Unfortunately, not many phone manufacturers support CyanogenMod and therefore she still has not purchased a new phone.

But the main reason why students do not have an iPhone was the price. Nine out of the ten students mention cost or value for money and how it influenced their decision to purchase an Android phone. Students note that they had a strict budget, and that they wanted something inexpensive and did not feel the need for the latest model. Some students bought a used phone or received one as a hand-me-down from a relative or friend. Saskia used to own a Samsung phone, but finds them too expensive nowadays and has switched to a cheaper Huawei. In her opinion it is very similar, but she is less worried about the possibility of it breaking since it is not as expensive. She prefers her Huawei now because it does not have as many preinstalled Samsung apps (so-called bloatware) and services.

Correlating the variable smartphone adopter and mobile phone attitude category, four out of ten of the students meet the criteria for late adopters.

> I refused to have one, I resisted getting one for a long time because I tend to get easily distracted, and I think having a smartphone brings out the worst in me.
>
> *Ich habe mich sehr lange gegen die Smartphones gewährt, weil ich weiß, ich kenne mich ganz gut mit sowas, ich lasse mich super gerne ablenken von Dingen, und da ist das Smartphone, glaube ich, das Schlimmste was einen passieren kann." (Beate)*

Jörg, the laggard smartphone adopter, says:

> Moreover, my point of view used to be: I am already studying library and information science and I am on the computer all day; at home, one of my hobbies is my computer — I really don't need to stare at my mobile devices during my half hour commute by subway or bus.

[23] https://support.microsoft.com/en-us/help/4485197/windows-10-mobile-end-of-support-faq
[24] https://www.androidauthority.com/cyanogenmod-lineageos-654810/

Ich studiere sowieso Bibliothek- und Informationswissenschaft, ich bin an Computern selber zuhause sowieso auch interessiert als Hobby, ich arbeite auf Arbeit an einen Computer, das heißt, meiner Ansicht nach bin ich den ganzen Tag sowieso schon von Computern umgeben, wenn ich jetzt nochmal eine halbe Stunde Bahnfahrt oder eine Stunde Bahnfahrt nach Hause oder sonst wohin habe, bin ich der Meinung, muss ich nicht unbedingt auf das Smartphone gucken.

Some of these students remark how cost-efficient the switch to a smartphone has been. They do not have to pay for text messages anymore, since they've switched to messenger apps as a means of communication.

Regarding students' memories about their first smartphone, two students (Ralf and Florian) confess that, initially, they felt overwhelmed.

Florian only had it for a few months but never really felt comfortable using the touchscreen and also thought that the mobile operating system had not fully matured. He acknowledges his struggle to adapt to it and how he soon lost interest. He went back to a "dumbphone" for quite some time.

Ralf compared his first few weeks with his first smartphone (2015) to how his parents behave with their computer.

> I felt somewhat like my parents must feel when I explain how to do something on their computer.
>
> *Ja, ich habe mich so ein bisschen gefühlt wie meine Eltern, wenn die vor dem Computer sitzen, und ich denen irgendwas erklären will.*

Noting how "cool" it was to have access to mobile internet and all the apps is another phrase that students relate to their first smartphone.

Elke confesses that although initially receiving emails on her phone was fun and convenient, she thinks that her phone can be a burden now, too. Now she uses it all the time as her alarm clock, to check her work email first thing in the morning, and to procrastinate.

Jörg, the smartphone laggard, claims that he instantly fell in love with his phone – finally, he was able to communicate quickly via messenger apps. For Saskia, it was not really a big deal since everyone in her class had one and then she got one too – she says that she just grew into it.

7.3.2.2 American Students

Out of the ten students interviewed, only three had an Android. Harper chose Android phones because she does not like Apple as a company. Owen and Ryan both like being able to customize their phones and get into its "guts." Owen used to have an iPhone but he always jailbroke it, which in the end became very tedious. He also has his current Android phone rooted,[25] and finds that it accomplishes lots of things that an iPhone can't. He demonstrates this by showing how he has customized his headphones. His headphones do not have a volume control, but he was able to customize it via an app, which, according to him, is not possible on an iPhone.

Harper and Owen point out they primarily utilize the Google ecosystem. Having a Google phone makes more sense to them in terms of connectivity and transferability with all Google services. Harper declares, "I love Google, everything I do is on Google, I use Drive, I use Google Photo."

Out of the seven remaining students, three students are late majority smartphone adopters. Marsha wanted to have an iPhone because she used to have one for work, so there was less of a learning curve. Moreover, her boyfriend had one already, so if she needs help, she can rely on him. Luke had never had one before and switched from Android to iPhone and now loves it. He also thinks that most Americans own an iPhone. Ava never had an iPhone, but all her friends had one. She says that the iPhone is supposed to be the "cool" gadget: the apps are cooler and it is harder to steal. Now she really loves it. The remaining students are iPhone users for various reasons: Liam always had an iPhone and does not like Android; Abigail always got iPhones from her parents. She also noticed while traveling abroad that more people had Android phones and how interesting it is to her that while in America everyone wants the new thing and the cool thing, it differs when you are abroad. Jack and Steve both like its interoperability with iTunes. For Jack, being able to connect his iMessages with his MacBook is another strength that makes the iPhone superior over Android devices.

Reminiscing on their first smartphone, early adopters like Liam noted how cool it was upgrading from a flip phone to a touchscreen phone and how friends were jealous of him. Steve paused for a brief moment and then told me that it made him feel like a grown-up. Most

[25] https://www.androidcentral.com/root

of the early majority smartphone adopter students remembered how much fun it was to have access to apps, a camera, and internet on the go. Of the two late majority adopters, Ava felt excited and also relieved because she finally could answer emails while out and about. She was less worried about being away from her laptop. Marsha disclosed that some things changed slowly; for example, she did not use maps a lot at first because she was not accustomed to having GPS.

7.3.3 Privacy Definition

Privacy as a concept covers a wide range of topics. Chapter 3 depicted privacy from different disciplines as well as a cultural perspective. Below, study participants share their thoughts on it.

7.3.3.1 German Students

Several students said it is a difficult question to answer since it is such a broad topic. Nonverbal cues that signified this included long pauses and nervous laughter/chuckles. For example, Ute is startled and admits, "... phew, oh well, oh god, it is, I don't think I can come up with an answer spontaneously, I never ..." *("… phew, ja, oh Gott, das ist, da kann ich jetzt gar nicht so spontan eine Antwort darauf geben, habe ich noch nie so ...")*

After a long pause and some hesitation, Florian said he is unable to come up with a textbook definition. According to him, privacy is deciding what he divulges and what he does not. It can be any information related to himself, such as things he is embarrassed about, such as how much electricity he uses and what kind of medication he takes.

> All the things related to me, things, that, if other people would know them, could also harm me; and that I make the decision [regarding] what I reveal, if [anything] — that is privacy for me.
>
> *Alles Dinge, die mich betreffen und deren Wissen anderen dazu verhelft, mir schaden können, essentiell schaden zu können; dass die Entscheidung bei mir liegt, wann und wie ich sie preisgebe, wenn überhaupt, das ist für mich Privatsphäre.*

Saskia mentions that the loss of privacy is both scary and dangerous. She states that without privacy, she could not do anything without being watched — which is dangerous since people would know when she is not home and could easily break into her apartment. Privacy signifies the ability to remain anonymous about her whereabouts and what she does.

Some German students bring about the concept of privacy as a "physical place." It is their home, where they can close the door, shut the curtains, and retreat from the outside world – their physical sanctuary, as Jörg states: "well, privacy is when I come home and close my door – then I am private." *("also Privatsphäre ist schon für mich schon alleine, wenn ich nach Hause komme und meine Türe zu mache, dann bin ich privat.")*

Defining privacy as being the opposite of "public" is mentioned by Beate, as is the danger of publicly posting something at one point because the internet does not forget.

> It kind of sucks, if the internet knows, one cannot deny that it ever happened or say, "Well, that was a long time ago."
>
> *dann ist es natürlich Scheiße, wenn das Internet das weiß, weil dann kann man es nicht abstreiten, man kann auch nicht sagen, das war einmal.*

She continues by talking about personal health information and how important it is to have the right to privacy regarding personal health. Health data is something two other students mention (see also Florian in the paragraph above), with Berthold emphasizing how important it is to have personal health information safeguarded by privacy.

Two students talk about the idea of "Big Brother is watching you," but from different points of view. For Heike:

> It feels a bit creepy, a bit "Big Brother is watching you": I always used to say, "I don't care because I have nothing to hide,'" but then I found out that is a common saying uttered by many people, but, of course, that doesn't mean you want the entire world to read your emails.
>
> *[Es] fühlt sich einfach so ein bisschen gruselig an so "Big Brother is watching you" Ding ... früher habe ich immer gesagt, ach ist mir doch egal, ich habe eh nichts zu verbergen, wie ich mittlerweile rausgefunden habe, so ein Standardsatz von den meisten Leuten, aber natürlich möchte man trotzdem nicht, dass die ganze Welt deine E-Mails lesen kann.*

She further confesses that even though, in theory, she finds the idea of being surveilled scary, in reality, she does not protect her privacy as much as she should. Some of her friends use Fairphones,[26] but she thinks it is too much work to use these kinds of phones.

Ute's perception is the opposite:

[26] see https://www.fairphone.com/en/. However, these phones are not better at protecting a user's privacy

> Well, I sorta feel like someone is always watching — that idea is a bit exaggerated, I don't mind it too much.
>
> *Ich finde diese Bilder, dass irgendwer zuschaut, finde ich eh immer ein bisschen fehl am Platz, also ich habe jetzt eigentlich nicht so viel dagegen.*

Ute does not mind if her search history is analyzed, as long as it is "just" documented in a big server or computer. However, she adds that if humans, insurance agencies, or the government had access to her data it would be horrible. Interestingly, she also had real difficulties defining the concept of privacy.

Berthold, Jörg, and Wolfgang already relate to privacy in a digital context such as the internet, apps, and social media. Berthold thinks:

> Outside of the internet, one knows how to protect one's privacy, be it by sending a postcard or a letter, or whether one closes the curtains or not.
>
> *Außerhalb der der Internetnutzung weiß man gut, wie man seine Privatsphäre schützen kann, ob man jetzt eine Postkarte verschickt oder einen Brief und ob man am Fenster die Vorhänge zu macht oder nicht.*

Elke connects privacy to mass surveillance and the cooperation of secret services such as the US's National Security Agency[27] and the Bundesnachrichtendienst (BND).[28] According to Elke:

> Well and I would consider it an invasion of my privacy, if they [secret service] would know that I sent a message on a specific date and time – even just the metadata.
>
> *Aberr ich fände es schon, also ich würde meine Privatsphäre schon dann verletzt sehen, wenn nur, wenn die [der Geheimdienst] nur wissen würden, ich hab am den Tag zu der Uhrzeit der und der Person eine SMS geschrieben – nur die Metadaten.*

7.3.3.2 American Students

Several American students are puzzled by the privacy question and had difficulty answering it. I observed many nonverbal cues while students answered. Long pauses, nervous laughter, hesitation, filler words such as "umm" and "hmm" emphasized how much difficulty they had responding. Harper declares:

> Um (…) so, I think privacy is very tricky, because privacy to me is making sure that the things that I want to, that whoever I want to see these things sees them, but to people that I don't want them, that they don't see it … sensitive information to me is obviously

[27] https://www.nsa.gov/

[28] https://www.bnd.bund.de/EN/Home/home_node.html

> things like Social Security number, bank account information, but it is also things that are personal so, like, sensitive information can be things about myself that I don't want to tell people (…) However, it becomes tricky if you because with social media you are able to put so much out, and sometimes you forget that other people have access to it. I guess, it just privacy is just the general sense that people should know what you want them to know, kind of thing, and no more and no less, so even if you said something publicly, if you don't want someone, someone saw it, that you didn't want them to know it. Technically, that is not a privacy breach, but like to me that *would* be a privacy breach, just because that is how I view privacy.

Jack views it as:

> To me, privacy is just like [being in the] bathroom: to be not watched when I am peeing, like the right to hold my phone and just like no one looks at it, that is privacy to me. But big companies collecting data on me, I don't really mind that, that is just, they have the right, well they don't have the technical right, I don't mind them using that/their data for their good to get bigger, because they are collecting information from a bunch of people, so my data is just small compared to everybody else, it is a lot of information out there, so it is not that they are going to use that data for bad. It is just when individual people collect data on me, I don't like that.

Out of the ten students, six (Ryan, Owen, Liam, Abigail, Luke, Ava, and Jack) linked privacy to the digital world, mentioning apps, the internet, and social media. As Luke says:

> Privacy is selecting what you want others to see, whether it's a friend or foe or just people or everyone, that has access to the app or website; it is what you want to show people and what you want to keep to yourself.

For Ryan, privacy is a crucial concept; even though he loves Google and lives in the "Googlesphere," he opted out of ad tracking. He did not want Google to analyze and profit from his online behavior.

Abigail and Luke relate privacy to danger, as an invasion of privacy can lead to stealing of Social Security numbers, financial information, and ultimately lead to identity theft.

Marsha and Ava consider themselves "open" people and do not mind sharing personal information about themselves at all. Nonetheless, in the same context, they both emphasize that it has to be their decision.

Luke is the only student declaring privacy outdated and essentially over.[29]

[29] However, Luke's comments on mobile privacy somewhat contradict his statement here.

7.3.4 Mobile Privacy Definition

Mobile privacy as a concept and as a reality is relatively new. The research question defines mobile privacy as "personal data and information being accessed or transferred onto mobile devices to device manufacturers, app developers, and other third parties."
German and American students' definitions are shared in the next sections.

7.3.4.1 German Students

Ralf and Elke flatly declare that mobile privacy is not possible. Ralf states:

> There are always going to be people, and it doesn't matter how well you protect your smartphone, they will be able to access it, if they want to. I am not saying someone is reading stuff on my [phone], but if I am a [criminal] suspect or there might be other reasons why they might surveil my smartphone, and they have the ability to do it, there is no real protection.
>
> *Es gibt auf jeden Fall immer Leute, die werden, egal wie gut du dich schützt, mit so einem Smartphone darauf zugreifen können, weil die also, wenn es jemand möchte, sage ich mal so, also ich behaupte jetzt nicht das jeder mein Handy liest, aber im Fall dessen ich werde wegen irgendetwas verdächtigt oder es gibt genügend Gründe, dass die mein Handy überwachen dann können, Sie es auch, da gibt es also keine wirklichen Schutz.*

He adds that the only way to guarantee mobile privacy is by "not using any smartphone at all [he is laughing]. Be 'off the grid,' just say, 'Hey, I don't need it.'" *("Kein Smartphone mehr benutzen [er lacht] 'also off the grid einfach sagen – hey ich brauch das nicht'.")*
Elke believes "that is nearly impossible, because independent from the operating system so many other stakeholders harvest your data" *("Also das ist für mich fast unmöglich, ehrlich gesagt, weil es eben, egal unabhängig vom Betriebssystem, gibt es so viel Akteure, die da Daten abgreifen.")* It would be a wish come true for her to find a:

> Data-secure, privacy-protecting mobile phone. Starting from the operating system to the app store of course, but all apps must be available, I find it extremely difficult [to find].
>
> *Ein datensicheres Privatsphäre schützendes Mobiltelefon zu haben. Aber genau angefangen beim Betriebssystem bis zum App Store natürlich, der trotzdem natürlich alle Apps bereithalten muss, finde ich es extrem schwierig.*

Another student agrees with her point of view: "The smartphone can reveal a lot of personal data, and you have to pay attention and if you have/want to maintain privacy, one has to do

the right thing." *("man an sehr vielen Stellen darauf achten muss, wenn man die Privatsphäre aufrechterhalten muss/möchte, dass man das Richtige dafür tut.")*

The physical aspect of the smartphone is something two students relate to the idea of mobile privacy: Beate would view it as an invasion of privacy if someone were to grab her phone and scroll through her photos. Wolfgang says mobile privacy encompasses not giving your phone to a stranger.

Florian correlates mobile privacy to having just a few apps installed, deleting unused apps, and being thoughtful about his app choices.

Jörg considers that:

> Privacy would also be the function within WhatsApp that lets you know if your message has been read or not. Everyone knows the game of, "Well you read the message an hour ago, why don't you respond?" To me, that is also somewhat of an invasion of my privacy …
>
> *Privatsphäre würde mich vielleicht auch … die Tatsache bei WhatsApp diese Funktion, das sofort sichtbar ist, wann Nachrichten gelesen wurden oder nicht, das Spiel kennt ja jeder: Du hast ja meine Nachrichten schon vor einer Stunde gelesen, wieso antwortest du denn nicht. Das ist für mich auch so ein bisschen der Einbruch in die Privatsphäre.*

7.3.4.2 American Students

As with the overarching privacy question, the subject of mobile privacy caused several students to pause for some time, to ponder and to ask for clarification.

Marsha admits that she does not have a good handle on the concept of mobile privacy and:

> (...) I don't know, um (…) because I still think of it as more of a phone than a computer, so it has information on it, but I still think of it like it is a phone and I make calls and I send text messages. Like, I don't think of everything else that's potentially on there or send from or to there, um (…) hm.

Abigail wonders if I mean cell phone privacy and Luke needs further explanation of what I mean and then proclaims, "That is a hard question to answer … I guess contacts is fine, that is being normalized already, but in terms of accessing my photos, my music, like overall data, that is an invasion of privacy."

Jack confesses:

> Hmm (…) I don't think I have any privacy in terms of the apps that I use; they collect a lot of information – they've got access to everything, they know more than my girlfriend, my parents though, to be honest. Yeah, but how do I feel about it? I think since we are talking about it, it is a little sketchy, it is a little weird but, in the moment, when I am using the app, I don't really mind.

Ryan refers back to his thoughts on privacy but also points out that mobile brings it to a different level. He brings up the security risk of using an open Wi-Fi and how it leaves one vulnerable to tracking and malware.

Ryan, Liam, and Steve define mobile privacy as controlling which apps, websites, or personal information is accessed on their phones. However, Liam claims:

> I know that the people who developed the phone or Apple, they can have access to whatever they want, really. Kind of scary but it is interesting, I guess.

Harper defines mobile privacy as other people not eavesdropping while she talks on her phone, not being able to read her text messages, or "not allowing the average person to access whatever is happening in here [she points to her phone] unless I give them [explicit] access to it."

7.3.5 Mobile Privacy Behavior and Attitude

Mobile privacy behavior is related to personal data and information being accessed or transferred from a smartphone to a device manufacturer, app developer, or third parties, as well as how a study participant utilizes smartphones, apps, and mobile websites in his or her everyday life. Findings are based on the experiment that investigated mobile privacy behavior from three different viewpoints:

1. participants' knowledge of, behavior with, and attitude with their own device;
2. downloading, installing, and trying out a specific app; and
3. behavior associated to the student's favorite app.

Mobile privacy attitudes include feelings, emotions, thoughts, positions, and established perceptions of study participants regarding various subtopics: location services, privacy policy, sharing of personal information and data, being a transparent human, and WhatsApp.

7.3.5.1 Mobile Privacy Settings Behavior and Attitude

This subchapter describes student's familiarity with their own mobile device privacy settings'.

7.3.5.1.1 German Students

German students' knowledge of and behaviors regarding smartphone privacy settings are substantial.

Elke says, "… I have to think about it, well, of course, when I select my apps." *("... Da muss ich mal nachdenken, also natürlich bei der Auswahl der Apps. ")*

Beate declares:

> I always have Bluetooth disabled, even though I am not sure it helps in terms of data protection. Well, and I always have security [she scrolls through her options and security settings] enabled, well remote access, sometimes I read about things and think that I don't want it [she smiles forcedly], even though I don't understand what it does.
>
> *Ich habe auch Bluetooth meistens aus, obwohl ich nicht weiß, inwiefern das Datenschutz an sich gut ist. Genau und sonst bei mir ist Sicherheit immer [sie scrollt auf geht auf Einstellungen unter Sicherheit], also der Fernzugriff, ich lese manchmal Dinge und denke, dass kling, als ob ich es nicht aktiv haben wollen [sie lacht etwas gequält], obwohl ich nicht weiß, was es macht …*

Florian encrypted his phone to protect his contacts, and:

> I don't know off the top of my head where I would find it now, but I searched for [the privacy settings] for a few apps. I configured data and Wi-Fi usage, which was because of high data usage, but there are a few apps, for some Samsung apps, I tried to prevent them from sending data. Well I am not sure, as just a regular user on this device, that these apps cannot send any data, I don't want that.
>
> *Ich habe auch bei einigen Apps, da weiß ich spontan nicht mehr, wo ich das finden würde, aber ich hab danach gesucht, einigen Apps habe ich mobile Daten und WLAN geregelt, das hatte mehr Trafik-Gründe, aber es gab auch einige Apps, bei Samsung eigenen Apps, die das Telefonieren nach Hause zumindest versucht haben, wissen tue das ja nicht genau als reiner Nutzer auf diesem Gerät, das die nicht nach Hause telefonieren, das möchte ich eigentlich nicht.*

Jörg shows the screen lock function but then admits to turning it off. He complains:

> I have to say, what I miss a bit in the context, when I think about it, is a kind of privacy function or privacy tab ... on a smartphone it is indeed, as you see, divided into tons of submenus and you have them here and there. There's something to adjust, it is relatively time-consuming because of all those submenus, and it is really not easy. And

then of course, if you are a bit lazy or not tech-savvy, you won't have it set up in like five minutes.

Was ich sagen muss, was mir jetzt so ein bisschen fehlt, wenn ich jetzt darüber nachdenke in dem Zusammenhang, ist wirklich eine Art Datenschutzfunktion oder Datenschutzreiter ... bei so einem Smartphone ist es ja, wie man sieht, auf massenweise Unterverzeichnisse aufgeteilt und man muss hier und da und dort mal was einstellen, es ist dann relativ, finde ich, zeitaufwendig, weil es dann auch öfter Untermenüs gibt, es ist nicht ganze einfach und das ist natürlich auch so, wenn man da ein bisschen faul ist oder nicht bewandert ist, hat man das nicht in fünf Minuten eingestellt.

Ute, Saskia, and Heike are not very familiar with the privacy settings on their phones.

Ute admits:

Generally, for the phone, [she touches her phone] I don't use settings a lot, um … [she scrolls and goes to settings] I don't know for sure, I mean, there are things that I, when I got it, I mean, I went through all the settings and reviewed everything, but now, well, I don't know anymore.

Ja, vom Telefon generell [sie geht auf ihr Handy] gehe ich nicht so oft rein in die Einstellungen da brr ... [sie scrollt durch das Handy und geht auf Einstellungen], weiß ich gar nicht unbedingt, das sind Sachen, die, also, als ich es bekommen habe, bin ich schon in das Menü mal durchgegangen und habe mir alles angeguckt, was es so gibt, aber das weiß ich jetzt eigentlich nicht mehr.

While Saskia muses:

I would go to settings, but I never thought about it [she scrolls to the settings on her phone and then to apps]. Apps, I am not sure if one can do it for the apps, maybe under permissions, maybe that way I can say, I don't want to allow that permission for each app. But I only just discovered it.

Ich würde einfach über Einstellungen gehen, aber ich habe noch nie so wirklich drüber nachgedacht [sie geht auf die Einstellungen im Handy, dann auf Apps] Apps, ich weiß nicht ob man das dann nach App machen kann, vielleicht Berechtigungen, dann kann ich vielleicht sagen, dass sie das nicht haben will, je nach App. Aber das habe ich gerade auch erst gefunden.

With Heike, I observe similar behaviors:

… [chuckling, touches her screen] I have to search for settings [scrolls through settings] … Well, here is something [she went to About the Phone] secure and reset. Well, I think that is only ... [she continues to scroll] as you can see, I am not too familiar with it [laughing, continues to scroll and search, clicks on Rules and Security] [a window with a number appears, she closes it] [she clicks on data protection and then on security]. Security and data protection [she clicks on it] …

… [leise in sich hinein lachend, tippt auf den Telefon Bildschirm], Muss ich selber suchen, Einstellungen [scrollt durch Einstellungen] also hier ist so eins [ist auf 'Über das Telefon'

gegangen], sichern und zurücksetzen, obwohl das ist nur … [scrollt weiter …] du siehst ich beschäftige mich nicht so oft damit [lacht, scrollt weiter und sucht klickt auf Regeln und Sicherheit] [ein Fenster mit einer Nummer erscheint, sie klickt dann wieder weg] [klickt dann auf Datenschutz und dann erscheint Sicherheit] Sicherheit und Datenschutz [klickt auf diese Einstellung jetzt] ...

Ralf, Wolfgang, and Berthold exhibit proactive mobile privacy behaviors.

Ralf quickly goes to his app permission settings, firewall settings, and anti-advertising software. He has his phone rooted and has installed CyanogenMod[30] on it, and:

> Then there are protected apps, that is pretty good. I am not sure if this is standard or because of CyanogenMod, but you can hide apps so they cannot be seen.
>
> *Dann haben wir geschützte Apps, das ist auch nicht schlecht, weiß ich nicht, ob das jetzt standardmäßig so ist oder wegen dem CyanogenMod, aber da kann man quasi Apps verstecken, dass man die nicht direkt sieht ...*

Wolfgang mentions app permission and notes:

> I actually review the permissions for each app that I am installing, and if it is possible to turn off settings that will prevent collecting personal data and information, well, then I turn them off.
>
> *Ich gucke in die einzelnen Optionen von Apps, die ich mir neue installiere, tatsächlich auch rein und, wenn es da Dinge gibt, die ich ausschalten kann, an denen was es an Daten über mich gesammelt wird irgendwie, dann mache ich das auch.*

Berthold talks about several settings, starting from app permission settings, guest user settings, having his phone encrypted, and having screen lock enabled.

> It is relevant for different things, not only if I give the phone to someone else, and here I can set up for each app the appropriate permissions, that is only possible since Android 6 and depending on the app you have to make a decision.
>
> *Das trifft ja dann auf verschieden Sachen, nicht nur, ob das Handy jemanden anderen gebe, also einmal kann ich hier in jeder App die entsprechenden Berechtigungen einstellen, das ist ja seit Android 6 möglich und je nach App muss man dann sehen. ")*

The majority of German participants have location services turned off by default, with Beate emphasizing, "what I notice right away is the GPS — I always have it turned off. " *("Also, ich weiß auf alle Fälle, was mir sofort auffällt ist die GPS, das habe ich eigentlich immer aus.")*

Some allow it for specific apps (Florian) or only turn it on when they need it (Wolfgang and Heike), with Wolfgang stating:

[30] https://www.androidauthority.com/cyanogenmod-lineageos-654810/

> So, I'll turn it on if I'm actually lost and need a map with my location, because otherwise I would be completely lost. Then I'll switch it on and let Google show me my location, just to know where I am, and then turn it off again.
>
> *Also, ich schalte es, wenn ich jetzt tatsächlich mich verlaufen habe und tatsächlich eine Karte brauche mit meinem Standort, wo ich mich sonst nicht zurecht finde, dann schalte ich es kurz ein und lass Google kurz mir meinen Standort anzeigen, damit ich weiß wo ich bin, schalte es aber auch dann wieder aus.*

Echoing Wolfgang's behavior, Heike declares she does not turn it on: "I open up the map and look at it … without the GPS. I really only turn it on when I'm completely lost [she laughs]." *("dann rufe ich mir die Karte auf und guck so. […] ohne das GPS. Also das mache ich wirklich nur, wenn ich ganz verloren bin [sie lacht].")*

Ralf tells me that there is one app that is allowed to track his location: Runtastic[31], the app he uses to track his daily running route.

> One can track how long one is running and I can track how long, how far I've gone … otherwise I do not use it. When I look at a map, I don't need it to show me where I am, because I know that I can find my way around the map.
>
> *Da kann man halt tracken [sic], wie lange man läuft, und da kann ich halt tracken, wie lange, wie weit ich gelaufen bin, und da mache ich es an, ansonsten mache ich es nicht, wenn ich auf eine Karte gucke, brauche ich kein Punkt, der mir anzeigt, wo ich bin, weil ich das weiß, ich kann mich ja an der Karte zurecht finden.*

7.3.5.1.2 American Students

The majority of American students are familiar with the privacy settings on their smartphones. Marsha acknowledges that she only became aware of the privacy menu on her iPhone because she took part in a five-day Privacy Paradox podcast challenge ("Privacy Paradox | the "Note to Self" Podcast Presents a 5-Day Plan to Take Back Your Digital Identity" n.d.). "I looked [at it] a little bit, but was not super fully in it, but it was in settings, and I think it was called privacy."

Owen does know how to find the permission settings for all of his apps. He explains how he can disable media, messaging, devices, and other permissions.

Harper immediately goes to the Privacy and Safety settings on her iPhone and says:

[31] Now adidas Runtastic

> Yeah, umm [she takes the phone into her hands] I think there is actually a thing; it is called privacy and safety settings [goes to it on her phone and shows it to me] of Android — whichever this one is [she laughs a bit].

She adds that some of her apps are password-protected:

> When you first open up the app, it immediately asks for a username and password … No, just for some of them, like my mobile banking or something like that, immediately it always asks for it.

Liam brings up Facebook:

> I am trying to think (…) like, for example, a lot of apps are using my Facebook [account to log in], and recently I looked up my Facebook to see how many apps use my or have my Facebook [login information].

All of these students admit that even though they are aware of various privacy settings, they are not actively perusing or using them.

Luke emphasizes:

> Yeah, but I hardly really do anything because I feel like the privacy bar is more like how you handle it, instead of how you manage it here [he refers to the menu]. Like how my behavior is, you know how, I feel like you don't simply give out your phone, that kind of thing. I feel that kind of matters more as opposed to managing it here.

Owen confesses, "I have looked into it before, but I am not too big on using it, only if I accidentally allow a permission." Ava has a similar behavior: "once in a while I go through it and double-check everything is what I need [it to be]."

Ryan struggles a bit in finding the app permissions settings saying:

> Oh man, apps with usage access [goes to settings, apps with usage access] … I usually would probably go just through search on the menu, but I happen to be in security, and it's got a couple of them listed here …

Abigail and Jack, both iPhone users, were not familiar with the privacy menu. Abigail knows where the Touch ID and security settings are but wonders where she would find the privacy settings. Jack bluntly asks, "Is there a privacy setting for that?"

One thing most all of the American students have in common is their behavior related to location services in as much that they all take some sort of action to control it.

Marsha says, "Umm, I know lot of people talk about the location services, so I set that up, umm." Harper states, "No, I always turn it off. I don't know, I feel weird about that. It sucks up battery I think, and I don't know why, but I just [turn] it off." Ryan allows it but adds:

> I don't have location turned on for all the apps; it is turned on for Google services, it is turned on for locate my phone, but other than that I don't think I have too many others that I give [location] access to.

Location services management differs among all students. Some have location services always turned on, allowing it for all apps, whereas some allow location only for specific apps, such as Google Maps. Some, including Marsha, make their decisions based on the app:

> I don't really need it to be on for Instagram, but it is kind of useful if I am using maps, to have location on so I tried to make (...) reasonable decisions to somewhat limit tracking.

Steve turns it on and off, because some apps will not work without it. Two students (Owen, Harper) have location services always off, only turning it on if they need it for specific apps or services, with Owen commenting, "For that I always have it off on my phone. [But] I don't deny the permission if I want to use Google Maps; I want to allow that permission."

7.3.5.2 Location Services Attitudes

As described in the previous subchapter, almost all students are aware of location services options on their smartphones. Furthermore, the majority of German and American students either disables location tracking completely or enables it only for specific apps. What are German and American students' reasons, feelings, and viewpoints offered for this behavior?

7.3.5.2.1 German Students

The majority of German students do not want to have their locations to be tracked. For example, Beate argues:

> ... Well I believe if I always have location services enabled, then it is easy to find out where a person works, lives, and does his/her grocery shopping, and maybe where his/her friends live, and [anything] else. I don't think this is necessary.
>
> *…, Weil ich schon glaube, wenn man sein GPS die ganze Zeit anhatte, könnte man aus den GPS Daten ziemlich gut raus lesen, wo dieser Mensch arbeitet, wohnt, wo er einkaufen geht, wo er vielleicht auch seine Freunde hat und sowas, und das muss nicht sein.*

Wolfgang doesn't want his location data collected:

> Theoretically, if it is not turned off, it is possible to see where I am and where I am going. I really find that creepy; it is like someone is always watching me.
>
> *Also, zum einen kann rein theoretisch, wenn man es halt nicht ausstellt, immer geschaut werden, wo ich bin und wo ich mich hinbewege, und das finde ich halt tatsächlich wirklich creepy [sic], das ist so als ob mich jemand verfolgen würde die ganze Zeit irgendwie.*

Jörg, Heike, and Elke do not wish to be surveilled at all times either, as they would like to keep their locations private. For Jörg, it is:

> Because I think I don't necessarily need to be located, I don't want to be located … I don't want to be tracked, and I don't have to.
>
> *Weil ich denke, dass ich das nicht unbedingt brauche, dass ich geortet werde, ich möchte es nicht, geortet zu werden, … ich möchte nicht verfolgt werden, muss nicht sein.*

Some students' express confusion when it comes to location services (Ralf, Saskia, Heike). Ralf admits that even though he always has location services turned off:

> And these constant location accuracy improvement pop-up messages[32] from Google ... I cannot turn it off, I was looking for it, and they ask again and again. I don't know why? Maybe one day I will give in, but I won't do that [he is laughing], because I believe it is unnecessary.
>
> *Und diese Standortsverbesserungsgeschichte von Google, die es gibt, das kann man auch nicht abstellen, ich habe auch schon geguckt, die fragen immer wieder, ich weiß nicht genau warum, ich glaube, damit man irgendwann nachgibt, aber da weigere ich mich halt strikt [er lacht], weil ich, das ist halt unnötig.*

Saskia ponders:

> However, they seem to know [my location] anyway. This morning I took a photo inside my apartment while on my Wi-Fi, and ten minutes later I was asked if I wanted to upload the photo to Google Maps for Aldi[33], because I live next to Aldi. So people know what Aldi looks like … well, they must know my whereabouts. I really find it a bit strange when I get asked about it.
>
> *Aber man weiß es scheinbar trotzdem immer, also heute Morgen habe ich ein Bild gemacht in meiner Wohnung von der Verbindung, dann hat er mich 10 Minuten später gefragt, ob ich das Bild hochladen auf Google maps [sic] für den Aldi, der direkt neben meinen Haus ist, damit Leute wissen wie der Aldi da aussieht, also der muss zumindest*

[32] Similar to here https://androidforums.com/threads/improve-location-accuracy-pop-up-plaguing-me.1286671/

[33] A discounter grocery store

wissen, dass ich da in dem Umkreis stehe, das finde ich immer ein bisschen komisch, wenn er das fragt.

Heike assumes that even though she has location services disabled all the times, she still could be easily located: "They could probably figure it out anyway [we both laugh]." *("Würden die wahrscheinlich trotzdem rausfinden [wir beide lachen].")*

For Berthold, it is difficult to figure out what each app is doing with his location data, and he admits the challenge controlling how his location data is disseminated.

> Well, generally, I cannot control what each app would actually do with my location data.
>
> *Ja, weil ich ja generell nicht kontrollieren kann, was jetzt welche App mit dem Standort machen würde.*

Jörg also admits that it is difficult to pinpoint which companies are collecting his location data as it is:

> [smiling] Not specifiable, [continuing] I adamantly do not want third-party applications to gather his location data as, in my opinion, third parties do not need to know my location, they don't have to know it.
>
> *[er schmunzelt leise] Das ist nicht spezifizierbar.* [Und weiter vehement] *Also Dritte haben eigentlich meiner Meinung nach nichts mit meinem Standort zu tun, das müssen die nicht wissen.*

Two students oppose Google and other services' ability to track their location (Beate, Elke), with Elke stating:

> Well I don't want an enormous conglomerate such as Google [following me]; they are already collecting enough information through cookies and trackers on me, I don't want this corporation collects my location data as well.
>
> *Ne, also gerade so ein riesigen Konzern wie Google, der eh schon unglaubliche viele Daten bestimmt durch andere durch cookies und tracker von mir hat, da möchte ich nicht, dass da auch noch Daten gesammelt werden, wo ich mich gerade aufhalte.*

Saskia admits that she is less concerned about protecting her location privacy than about battery usage. She wonders:

> Because I am not sure if it drains battery, well and yes because you can be located, that's somewhat less of a concern to me, because you can be tracked via Wi-Fi and the other internet [services]. They always know one's location anyway.
>
> *Weil ich nicht sicher bin, ob es Akku zieht, gut und ja man damit geortet werden kann, das ist nicht so eine große Sorge von mir, weil man über WLAN auch über das andere Internet wissen die eigentlich trotzdem genau, wo man ist.*

7.3.5.2.2 American Students

American students are also concerned with location tracking. Harper and Liam do not want their location to be shared all the time. Harper admits that location sharing has:

> Always been ingrained in me; people shouldn't know where you are at all times … I feel like, I don't know, like my parents, [she is laughing] that is like a weird thing. I was never raised [as though] people should know what you are doing at all times.

Luke does it as a precaution and because he feels safer if his location is not shared without his explicit permission. Ava also mentions safety as one reason why she is mindful about sharing her location. She does allow it for certain apps, but she will not post her location to social media sites since she could become an easy target for a stalker.

Ryan says that:

> They want to be able to collect everything from everyone all the time. Why would you need that? It is scary that it is out there, that they're building the capacity to be able to monitor everyone all the time. I don't know …

Marsha tries to strike a balance between the convenience of having an app track her location and perhaps helping her finding her whereabouts versus her decision to limit location tracking in order to protect her privacy. She admits that:

> […] Even if I my location service is off they can figure out where the Wi-Fi or where the internet connection is coming from. They can figure out where I am.

Some students (Owen, Abigail) primarily limit tracking to save battery charge and not because of privacy concerns:

> Because it drained my batteries more, I do it more in terms of to save batteries, because this phone goes from 80% to 50%, I did it more to save battery.

Steve is also more concerned about his data usage and not his privacy, and therefore he has it turned off.

Jack is the only student who does not care at all that is location history is tracked. He is an avid Snapchat user and "that is a good thing because now I have geotags [laughing] … Yeah, I like geotags."

7.3.5.3 App Experiment: Perfect Piano Behavior and Attitude

As of August 2019, users have the choice of 2.46 million apps in the Google Play store or 1.96 million in the Apple App Store (*Annual Number of Mobile App Downloads Worldwide from 2016 to 2019 | Statista 2020*). What behaviors and attitudes do students exhibit during the download, installation, and try-out processes of the Perfect Piano app?

Note: the purpose of the download experiment was not to compare iPhone versus Android users. It was instead to observe user behavior and attitude in relation to mobile privacy issues.

7.3.5.3.1 German Students

Before downloading and installing the Perfect Piano app, several students (Ralf, Wolfgang, Ute, Berthold, Elke) skim through the reviews of the app in the Google Play store.
Wolfgang says that he reads through the reviews not so much to find out about security concerns, but to find out whether the app does do what it is supposed to do:

> I actually look at the comments — not because I am worried about security, but more so because I want to know if the app does what it promises. Sometimes, though it is pretty rare, something is mentioned about security, and then I search through the first comments to see if they mention something. But that is an exception.
>
> *Aber Kommentare gucke ich mir tatsächlich an, wobei es dabei nicht um irgendwelche Sicherheitsaspekte geht meistens, sondern darum, ob die App das tut, was ich von ihr will. Irgendwie, also ganz selten taucht da auch was mit Sicherheitsbedenken auf und dann recherchiere ich nochmal richtig in den ersten Kommentaren, wenn das was drinnen ist, das ist aber eine Ausnahme.*

None of the German students scrolled further down to look for and or to read the app's privacy policy. Offering feedback on why she is not reading or actively looking for the privacy policy in the Google Play store, Beate states, "I don't read the conditions of the privacy policy. That's a fact: one doesn't read privacy policies." ("*Ich bin auch kein AGB Leser, so ist es halt auch, man liest ja auch einfach keine AGBs.")*
Ralf[34] discloses, "I only looked for the permissions details, I did not look for the privacy policy." *("Ich bin nur auf die Berechtigungen Details gegangen, war nicht auf der Datenschutzerklärung.")*

[34] He made this comment during the debriefing session.

Some students (Ralf, Beate, Wolfgang, Ute) searched for and read the permission description in the Google Play store before they pressed the install button.

Wolfgang states:

> At first, a pop-up appears [detailing] the permissions for the apps – only a few apps don't need any permissions, those are my favorite ones. Well, I don't have an example right now, but there have been some apps I didn't install because of the [required] permissions; allowing access to these things for the app didn't make any sense.

He adds:

> … Many apps [ask for] permission to access one's contacts, and that is something I allow, even though I don't like it. Most apps don't need this permission [to be granted] to run smoothly, and well, a similar thing is that for many apps, one doesn't need to register with an extra account, one can just use one's Facebook account.
>
> *Dann kommt halt als erstes so eine Anzeige, welche Berechtigung die App benötigt, die wenigstens App brauchen keine Berechtigungen und das sind mir die liebsten tatsächlich ahm und ich habe tatsächlich kein Beispiel parat, aber es gibt Apps die nicht installiert habe, weil die Rechte, die da gefordert worden sind von der App einfach keinen Sinn machen. Und er gibt zu viele Apps die Möglichkeit bieten, automatisch die eigenen Kontakte einzuladen, und deshalb ist das halt eine Sache, die ich in Kauf nehme, obwohl sie mir eigentlich nicht passt, die meisten Apps bräuchten das für ihren Funktionsumfang nicht, und genau, was auch noch so Ding ist dabei, was irgendwie so ähnlich ist, es gibt relativ viele Apps, wo man sich nicht mehr selber registrieren muss, sondern sich über Facebook anmelden kann.*

Ralf does it because he:

> Want[s] to know, if I install the app, what does it get from me? Nothing in life is free [he is laughing somewhat artificially] … and I think, "Why does it need to access my files or my calendar," or whatever, and then I think, "Whatever; well then I won't install it."
>
> *Weil ich mir manchmal, ich möchte halt wissen [lacht etwas künstlich], was die von mir kriegt wenn ich die installiere ‚weil nix im Leben ist umsonst" [er lacht] … mir denke, warum brauchst du denn den Zugriff auf meine Daten oder auf den Kalender oder auch sonst, was denke ich mir so nö, also dann installiere ich die halt nicht.*

Some students (Beate, Ute, and Saskia) wondered why the permissions pop-up did not show up before they pressed the install[35] button.

Ute comments:

> In the past, it used to be that before you pressed install, permission details popped up. It's not like that anymore, I don't know why. So sometimes it is still like it and sometimes

[35] Depending on https://support.google.com/googleplay/answer/6270602?hl=en-GB

not, that's why I'm always looking at the permission details [she scrolls down] to see if the app just uses what it needs to work or if it wants to access other stuff, and in most cases, it doesn't pop up now.

Früher war es ja so, dass immer bevor man auf installieren gedrückt hat, diese Berechtigungsdetails angezeigt wurden, das ist jetzt nicht mehr so, ich weiß nicht genau, also manchmal ist es noch so und manchmal auch nicht, ich weiß nicht genau, nach welchen Muster das funktioniert, deswegen gucke ich schon auf die Berechtigungsdetails [sie scrollt runter], also ob die app nur das macht, was sie machen muss, um zu funktionieren oder, ob sie noch andere Sachen machen möchte, und in den meisten Fällen kommt dann noch, worauf das Ding zugreifen will, das kommt hier gar nicht zum Beispiel.

Berthold installed and tried the app for a bit and then went back into the Google Play store to read the permissions, "since I did not look at the permission, well I can look at the permissions now". *("Ja, also da ich mir das nicht angeschaut habe, kann ich mir natürlich noch anschauen, welche Berechtigungen diese App verlangt.")*

After installing and downloading the app, several students denied the app specific permissions. Below, some comments are highlighted, and are accompanied by images[36].

Student Ralf comments on the first pop up after he opens up the app (see Figure 8):

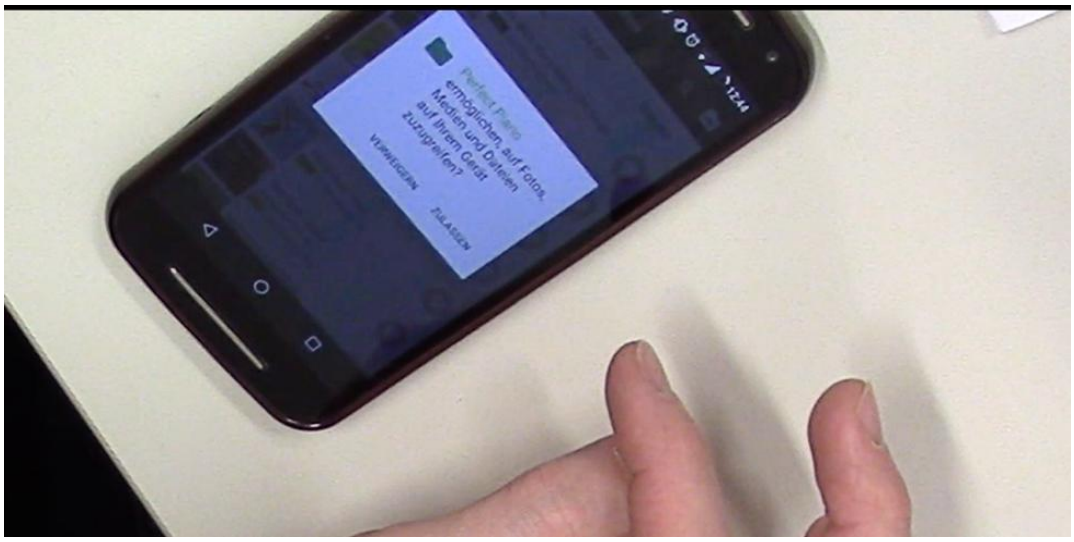

Figure 8 Image of Ralf's smartphone with first pop up from Perfect Piano app with pop-up: "Allow Perfect Piano to access photos, media and files on your device? Deny – Allow" *("Perfect Piano ermöglichen auf Fotos, Medien und Dateien auf Ihrem Gerät zuzugreifen? Verweigern – Zulassen")*

[36] All images are screenshots from the original videos; thus, the quality of them might vary.

Well here we go, [a pop-up appears – see photo in Figure 8 above] … I sorta don't know why it wants to access photos, media, and files. That's the question then: what's going to happen if I press deny? Well, I can try [he presses deny].

Da fängt es schon an [ein Pop erscheint – siehe Foto in Figure 8 oben*] da weiß ich halt nicht, warum um Fotos, Medien und Dateien, da ist halt auch immer die Frage was passiert, wenn ich verweigere, also man kann das ja dann ausprobieren [er klickt auf Verweigern].*

Then a new pop-up appears (see Figure 9 below). Ralf reads it and presses ok.

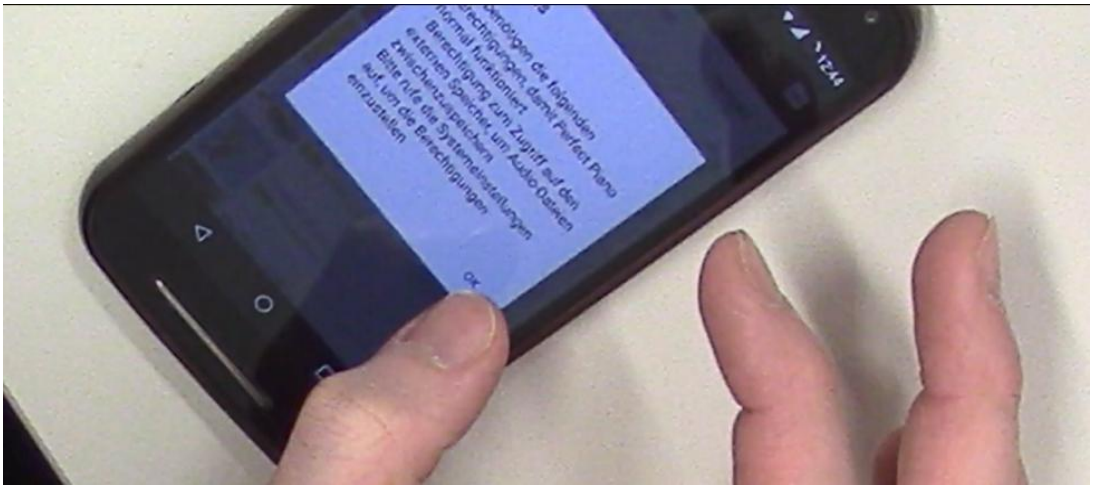

Figure 9 Ralf's smartphone with new pop up message from Perfect Piano app with pop-up: "requires the following authorization for Perfect Piano to function normally: permission to access external storage to cache audio files please go to system settings to authorize the permission." *("benötigen die folgende Berechtigung, damit Perfect Piano normal funktioniert: Berechtigung zum Zugriff auf den externen Speicher, um Audio-Dateien zwischenzuspeichern. Bitte rufe die Systemeinstellungen auf, um die Berechtigungen einzustellen.")*

He comments: "Oh ok, it wants to save it temporarily. Well, that's ok then" [laughing somewhat and then clicking on ok]. *("ach so, er möchte das zwischenspeichern, na gut, machen wir das so [er lacht etwas und klickt OK].")* Subsequently, another pop-up window appears, which he reads before pressing allow (see Figure 10 below).

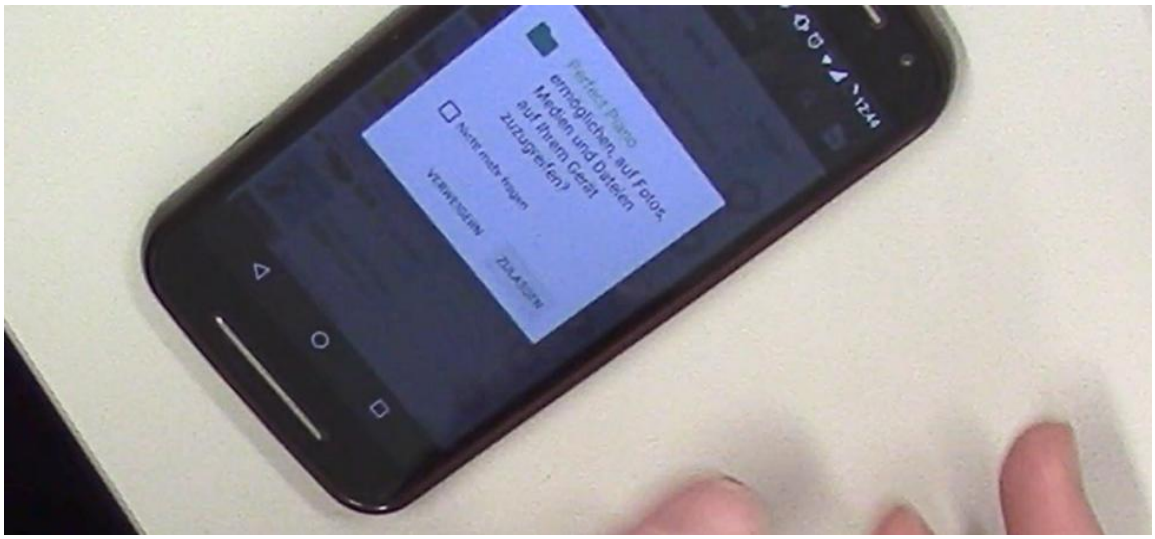

Figure 10 Ralf's smartphone with new pop up message from Perfect Piano app: "allow phone to access to photos, media and files on your device? c Don't ask again. Deny – Allow" *("ermöglichen auf Fotos, Medien und Dateien auf Ihrem Gerät zuzugreifen?* c *Nicht mehr fragen. Verweigern – Zulassen")*

Beate exhibits the following behavior while pointing at the pop-up notice (see Figure 11 below):

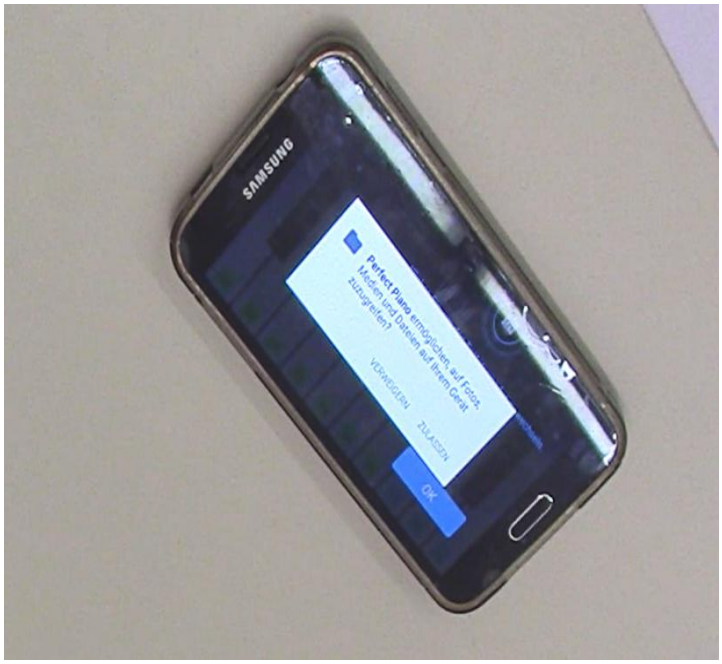

Figure 11 Beate's smartphone with pop up message from Perfect Piano app: "allow phone to access to photos, media and files on your device? Deny – Allow" *("ermöglichen auf Fotos, Medien und Dateien auf Ihrem Gerät zuzugreifen? Verweigern – Zulassen")*

So that's why I sorta get suspicious. Usually, if the app asks if it can access my media and files, well, usually I try to say NO, and sometimes the app functions without it, and sometimes it doesn't function without it, and then I weigh, "How urgently do I need the

app?" But usually my rule is to deny access to my media … well, for me that is the most personal thing on my phone … I think so, I mean, it is more personal to me than my messages [she clicks on deny].

Das ist halt das, was ich meine, also da werde ich immer ein bisschen spitzfindig, also in der Regel, wenn mich jemand fragt ob er auf meine Medien und meine Dateien zugreifen will, versuche ich immer erstmal zu sagen, NEIN, so, und die Frage ist manchmal funktioniert es auch ohne so und manchmal geht es auch nicht ohne, und dann schätze ich ab ok, wie wichtig ist es mir gerade, dass ich das wirklich haben will, aber in der Regel lehne ich gerade Zugriff auf meinen Medien halt ab, weil es halt das Persönlichste an meinen Handy ist, würde ich mal sagen, also ich glaube sogar manchmal persönlicher wie die Nachrichten, die ich da drauf habe. [Sie klickt auf Verweigern]

In the debriefing part of the interview she acknowledges:

That's the problem with transparency, and not understanding what it [the app] does: one downloads a keyboard app, and you understand if the app needs to use storage. But what about everything it [the app] actually can access and know, and nobody asks you about it, I mean one does not think about all the things the app can access, and then you think, "Wait a minute, why does this app store my photos?" Like, excuse me?

Das ist halt schon das, ist halt das Problem zwischen Transparenz und nicht wissen, was geht, du lädst dir halt eine Keyboard-App runter und denkst dir so ok, dass die meine Speicher zuspielt ist ja klar, aber, was da alles abgeht und was die alles weiß, weil auch dich auch niemand dazu auffordert, du kommst ja nicht auf die Idee, was die alles machen können, dann denkst du dir, "ja ok, wieso speichert meine Piano-App meine Fotos ab, Entschuldigung"?

Saskia reads the following pop-up (see Figure 12):

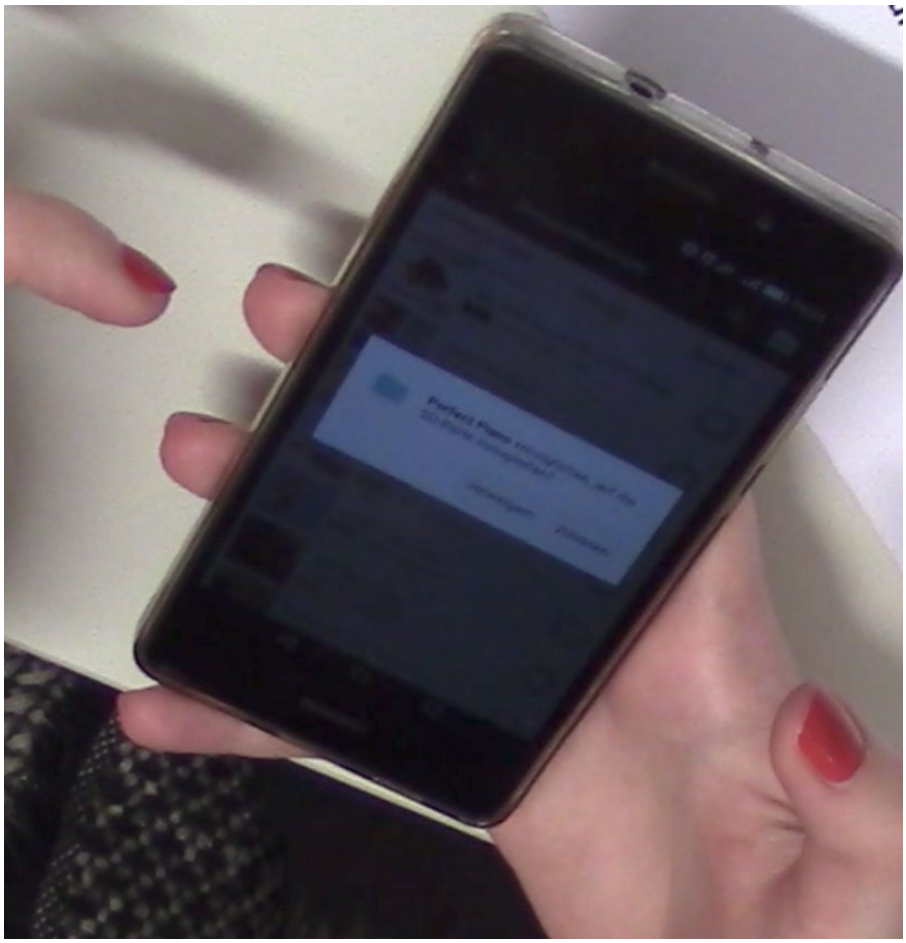

Figure 12 Saskia's smartphone with pop up message from Perfect Piano app: "allow Perfect Piano to access SD card. Deny – Allow" *("Perfect Piano ermöglichen auf SD-Karte zuzugreifen. Verweigern – Zulassen")*

Saskia's comments on it are the following (see Figure 12):

> It wants to access my SD card; finally, it asked me something [she clicks allow] and I think if I press deny, I cannot use it.
>
> *Er will jetzt auf die SD-Karte zugreifen, jetzt hat er mich endlich mal was gefragt. [sie klickt auf Zulassen] und "ich denke, wenn ich nein sage, könnte ich mir die Funktion nicht anschauen.*

After trying out the game for a bit, she remarks:

> well, it asked about the SD card; otherwise it didn't ask for anything else ... Well, I would say it doesn't have access to anything else.
>
> *also die SD Karte hat sie mich gefragt, ansonsten hat sie mich nicht gefragt und ich dachte, dass die sonst immer fragen ... Sonst würde ich sagen, hat sie auf gar nichts Zugriff.*

Heike demonstrates conflicting behaviors. At first, she wonders why the app needs access to her photos when the pop-up appears: "Allow Perfect Piano to access photos, media and files" *("Perfect Piano ermöglichen, auf Fotos, Medien, Dateien auf Ihren Gerät zuzugreifen* (see image above in Figure 11 (Beate)), but then she presses "Allow" *("Zulassen")*. Yet, she contemplates,

> If it wants … most of them want location, kind of photos or such things, and for apps, I wonder, "Why do they want that?" And then I gauge somewhat, "Do I really need the app?" But if I really want the app … oh well, then [I will] allow access to those things.
>
> *Ja, wenn die (...), die wollen ja dann meisten Standorte und irgendwie Fotos oder irgendwas und für Apps, wo man sich denkt, wozu brauchen die das, und dann überlege ich mir halt nochmal, braucht die App, also möchte ich sie wirklich haben und, wenn ich sie wirklich haben will, dann mache ich es halt trotzdem.*

Elke denies the permission to access media and data (see image above in Figure 12 (Beate)) several times, until she finally receives the following pop-up message (see Figure 13):

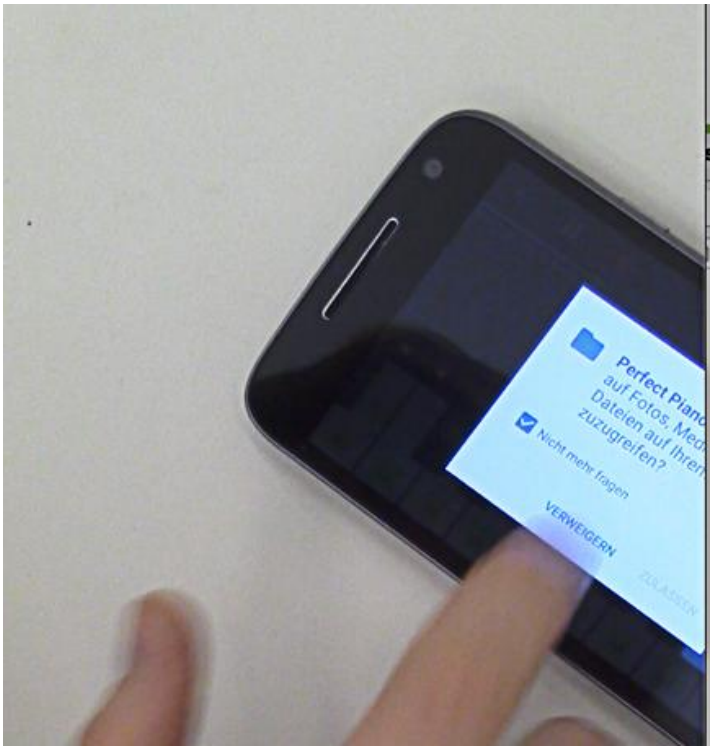

Figure 13 Elke's smartphone with pop up message from Perfect Piano app: "allow phone to access to photos, media and files on your device? Don't ask again. Deny – Allow" *("Perfect Piano ermöglichen auf Fotos, Medien und Dateien auf Ihrem Gerät zuzugreifen*? c *Nicht mehr fragen. Verweigern – Zulassen")*

She presses deny and clarifies:

> Photos and media, I don't know, it doesn't make sense to me. Why does the app need it? That's why I am going to press "don't ask me again."
>
> *Fotos und Mediendateien, das sehe ich, irgendwie für mich gibt keinen Sinn, warum diese App darauf zugreifen soll. Deswegen sage ich mal ok, ich will jetzt gar nicht mehr gefragt werden.*

7.3.5.3.2 American Students

Several American students (Owen, Liam, Harper, Abigail) read and commented on the reviews of the app before beginning the download process.

For Owen, the star rating system is helpful:

> Right [he went to the Google Play Store and looks for the app now] then I search for it, then I usually browse through the reviews. If I don't know the app and I see it has a 4.2 [stars] so I download it […] Yeah, I think my limit would be if I saw 3 stars, I would be suspicious, I'd probably think the app is useless, maybe I'll read through reviews and see if it says, "This app is bad it because it pops ads onto your screen."

Abigail also reads through the reviews:

> Sometimes, if I don't really know the app that well, I look for reviews and, like, the pictures to see if it is a trustworthy app or not. So […] I look through the reviews and if people, like, say a few bad things about it, I do further research on my own: I go to my web browser and look up the app and see if it is a legitimate app; there are spam and sketchy apps and such, so I usually just make sure to look it up first before I download anything.

None of the students searched for or read the privacy policy included in either the Google Play store or Apple's App Store.

Marsha admits:

> It is funny, I don't really ever look at the privacy policy but because this is what we talking about I am like, "I should open that," [says that in a louder voice] and I am, like, is that the bias? I guess I don't ever really look at it, so I am just going to click "get."

Liam comments on not reading a privacy policy before he downloads an app with, "nah, not when I am downloading an app, no."

As the majority of the American students own an iPhone, the download process differs from that of an Android phone. A user does not get asked to grant (or not grant) permissions before the installation process. Thus, all the iPhone users pressed the install button and then the app

downloaded.[37] After the installation process had completed, none of the iPhone users went into Apple's Privacy menu to review the access options for the app. Opening up the app for the first time, all iPhone users received a pop-up asking to allow or deny notifications (see Figure 14).

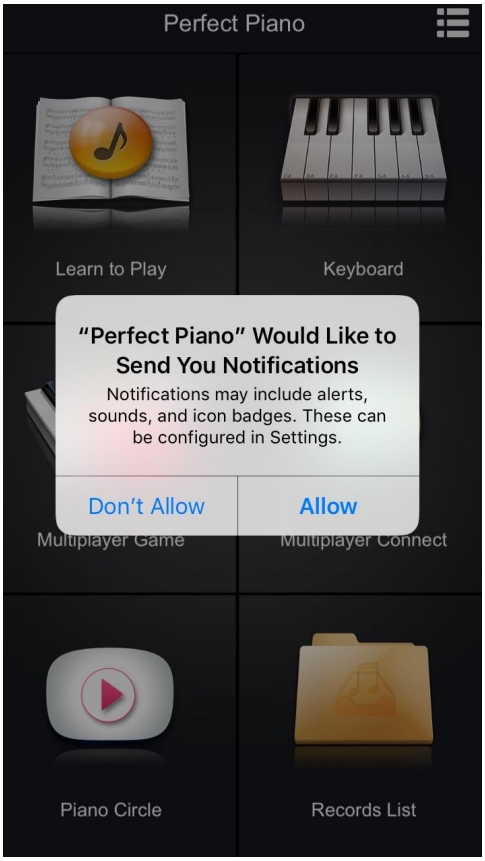

Figure 14 Perfect Piano app and Apple iPhone's typical pop up notification

None of the students allowed the app to send them push notifications, with Liam declaring "I usually [click] don't allow … because I don't want to see it all the time or it is not really relevant."

Jack tried out the multiplayer game feature in the app and quickly linked it to his Facebook account (see Figure 15 below).

[37] see also the explanation in discussion.

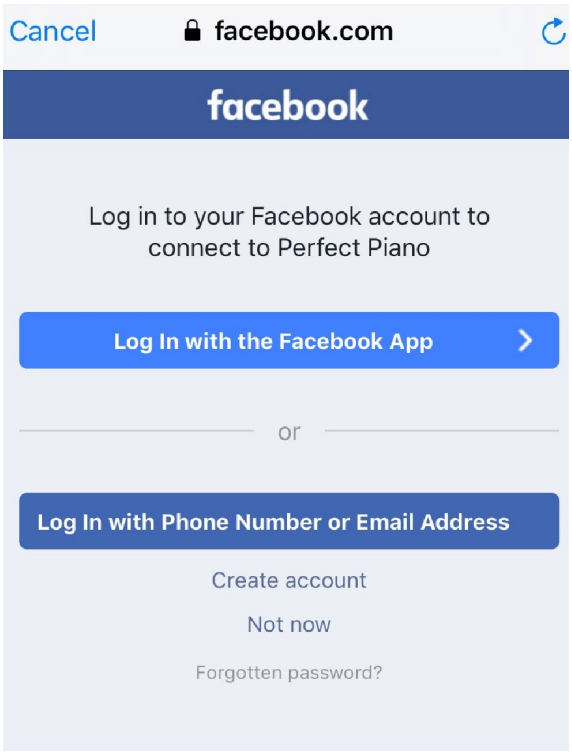

Figure 15 Screenshot of Facebook app account connection on Perfect Piano app

Jack then commented, "I am opening up an account with them using Facebook; it is a lot easier."

Out of the three Android users, two carefully reviewed the permissions of the Perfect Piano app. Owen ponders, he opens up the app, and a pop-up window appears (see Harper screenshot Perfect Piano permission in figure 16 below), "so, I see it is asking for access to my folders, media and files on [my] device — I don't know why it wants that, and I would, I feel like denying it. Am I allowed to do that?"

He then denies permission, but a few minutes later:

> [another pop-up shows up, he reads it, then the app opens, but then another pop-up appears] So, ok, it just explained to me why I need the permission: it said it needed access to my files, to my storage for audio cache. So now that I understand why it wants that permission, I allowed the permission now.

Harper remarked when the following message pops up (see Figure 16):

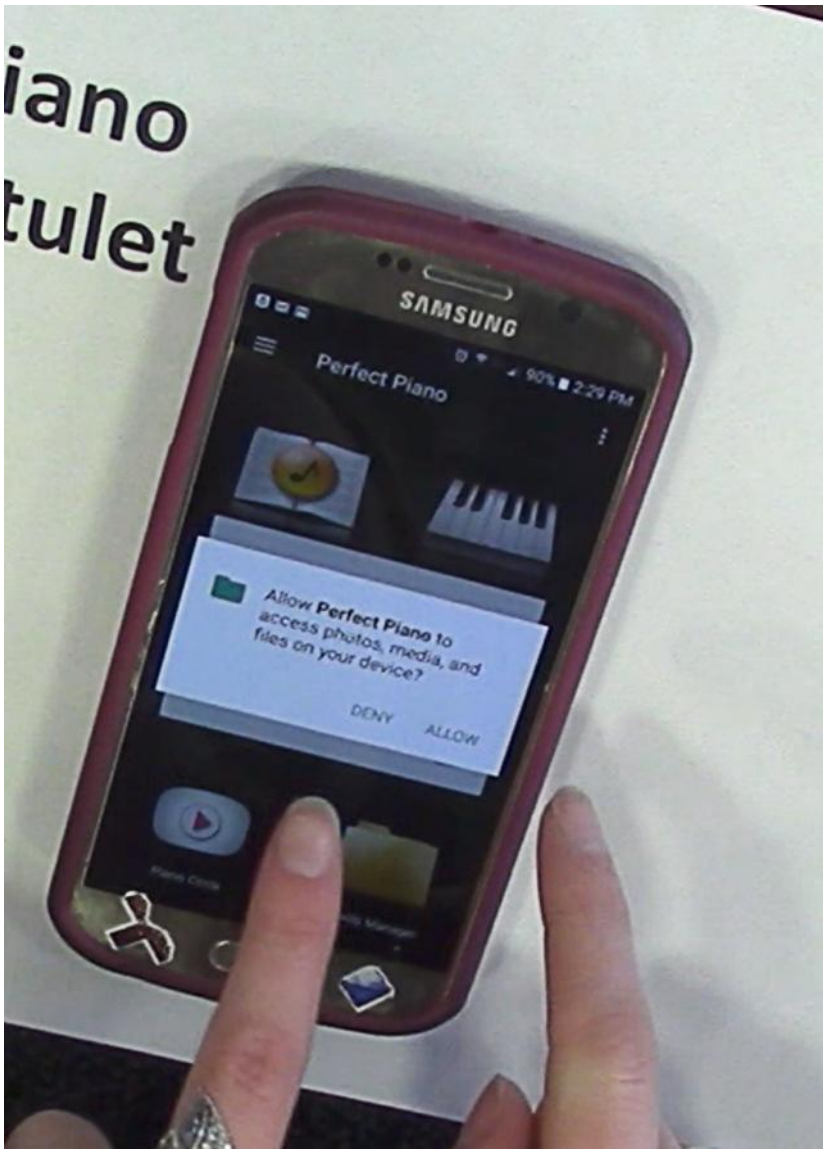

Figure 16 Harper's smartphone with pop up message:
"Allow Perfect Piano to access photos, media and files on your device? Deny – Allow"

"And then typically what I do [is] I press deny unless it says you cannot play this app unless [you press] allow." Then she presses deny, but moments later another notice pops up (see Figure 17).

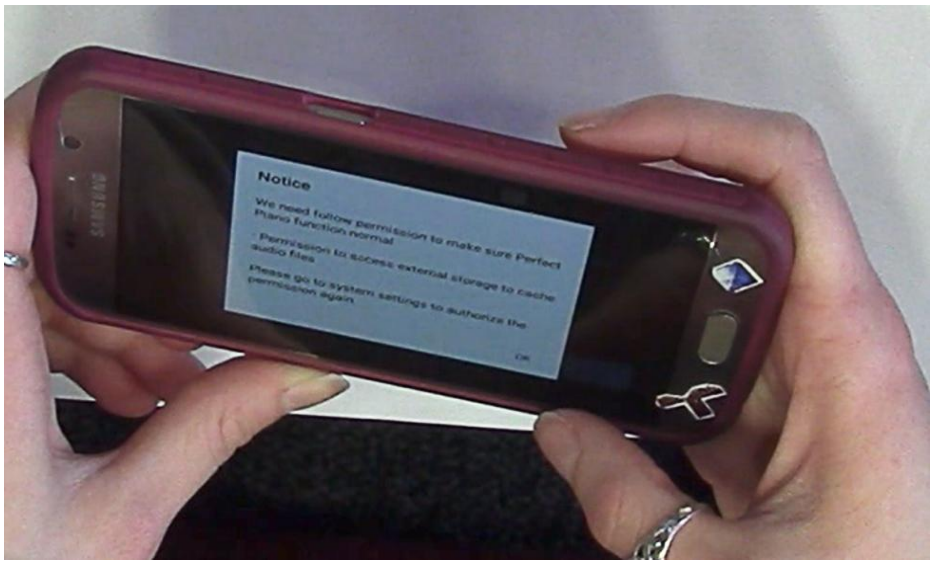

Figure 17 Harper's smartphone with new pop up message from Perfect Piano app: "Notice: We need follow permission to make sure Perfect Piano function normal. Permission for access to external storage to cache audio files. Please got to system settings to authorize the permission again."

She points out:

> honestly, at this point I would just uninstall the program […] there be like this is why you want it, to do things and if it doesn't say that, it is just kind of … OK, it says here "make sure it functions normal," like, what does that mean? They don't even [say], like, "If you want to know more, [visit] our website." It is just, like, "We need to function normal." What does that mean? I probably would uninstall it.

She uninstalls the app and says, "I don't like it if it makes me give it access to things unless it was a really, really good reason. Which is very hard for me … it would have to be a really, really good reason."

7.3.5.4 App Experiment Favorite App Behavior and Attitude

The following reports on students' mobile privacy behavior and attitude concerning their favorite app. Some of students' favorite apps were Facebook, Threema, WhatsApp, Instagram, Spotify and Snapchat.

7.3.5.4.1 German Students

Half of the participants (Ralf, Beate, Berthold, Jörg, Elke) are knowledgeable regarding what personal information and content their favorite app has access to.

Berthold discloses:

> Oh well, Signal as a messenger app probably has many permissions: for sure storage and camera and network and contacts, probably all the permission it can have, it has.
>
> *Ja Signal hat als Messenger-App schon ziemlich viele Zugriffe, ich, also Speicher ist sicher dabei und Kamera und Netzwerke und Kontakte, also wahrscheinlich fast alle Berechtigungen, die sie haben könnte, hat sie auch.*

Beate's goes to Telegram's privacy and security settings:

> Well and then, I always look into the settings to see what I can do about security and privacy.
>
> *aber sonst, glaube, gucke ich immer bei den Einstellungen zuerst nach, was ich Sicherheit und Privatsphäre, was ich also machen kann.*

The following image depicts it (see Figure 18):

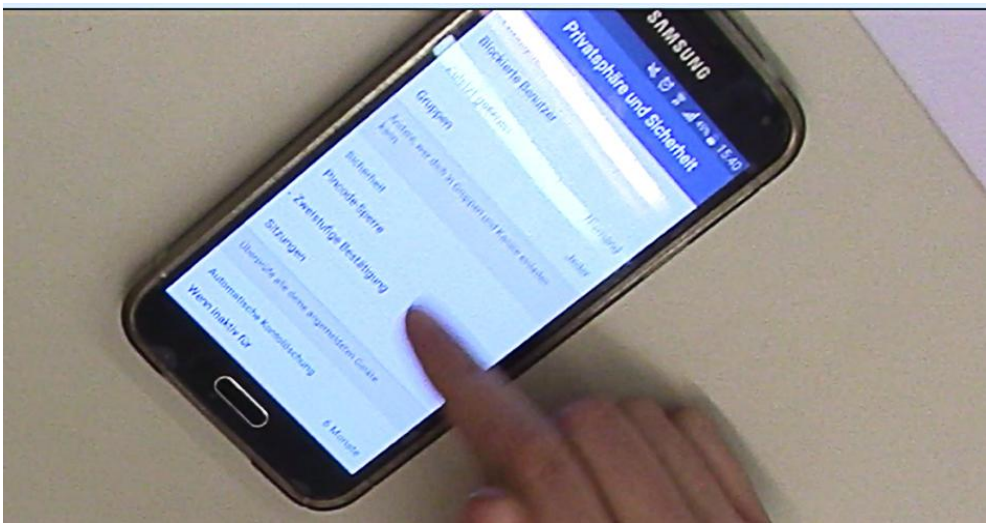

Figure 18 Beate's smartphone with Telegram app privacy and security settings: "Privacy and security: Blocked users / Groups: change who can reach you in groups and contacts. / Pin code locked / Two-level authentication / Sessions: Check all devices you are logged in. Automatic account deletion: If inactive for 6 months" *("Privatsphäre und Sicherheit: Blockierte Benutzer / Gruppen: Ändern, wer dich in Gruppen und Kontakte erreichen kann. / Pincode-Sperre / Zweistufige Bestätigung / Sitzungen: Überprüfe all deine angemeldeten Geräte. Automatische Kontolöschung: Wenn inaktiv für 6 Monate.")*

The other half, including Saskia, cannot remember and have to search for it: "well, I would go into settings, but I don't know anymore." *("Da würde ich wieder über Einstellungen gehen, aber weiß ich auch nicht mehr ...")*

Heike looks for it:

> Well, I don't know it off the top of my head, but I believe Facebook has access to everything, it always has access to everything … Well, I believe they have access to my personal information.
>
> *Also, so auswendig weiß ich es, glaube nicht, aber Facebook hat wahrscheinlich alle, die haben ja eh immer ... Na die haben bestimmt Zugriff auf meine persönlichen Daten.*

Heike finds the permission,[38] as the following images illustrate (see Figure 19):

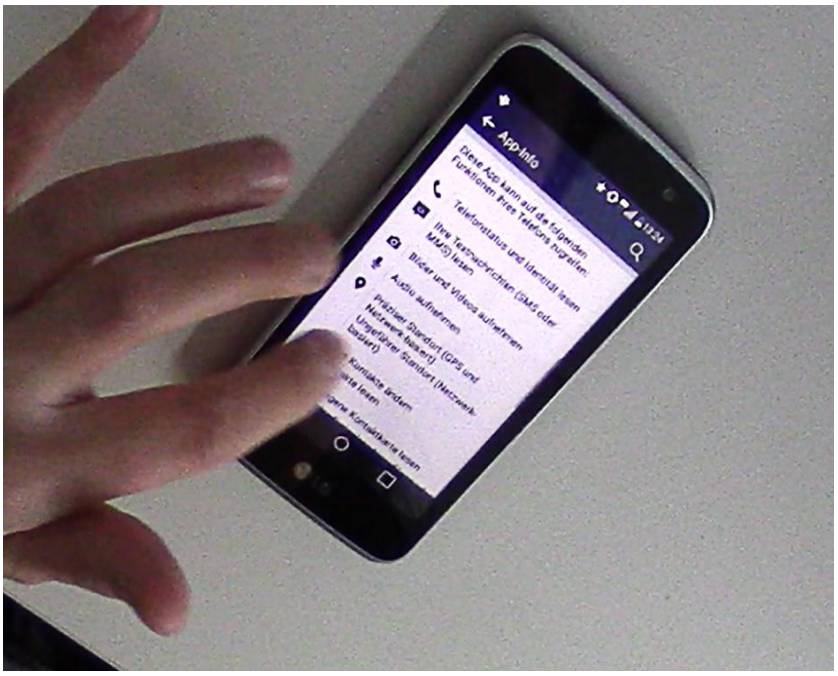

Figure 19 Heike's smartphone with Facebook app permission menu: "this App has access to device & app history/ read your text messages (SMS or MMS)/ take pictures and videos/ record audio/ precise location (GPS and network-based) approximate location (network-based)… add or remove contacts/…read your own contact" *("Diese App kann auf die folgenden Funktionen des Telefons zugreifen: Telefonstatus und Identität lesen / Ihre Textnachrichten (SMS oder MMS) lesen / Bilder und Videos aufnehmen / Audio aufnehmen / Präziser Standort (GPS und Netzwerk-basiert) Ungefährer Standort (Netzwerk-basiert) /…Kontakte ändern / … lesen) .")*

[38] But not the privacy policy.

Then Heike reads:

> This app [Facebook] has access to the following functions. Wow, that's quite something [she chuckles]: status and identity, read your text messages, that is new, if you have Facebook Messenger, then it shows your regular text messages, too. I don't want it, but I cannot change it. Photos and media files [she scrolls farther], exact location, contacts, email [she scrolls farther], they really have everything [she is laughing hysterically].
>
> *Diese App [Facebook] kann auf die folgende Funktion ihres Telefon zugreifen, oh ist ja krass oder [sie lacht lachen leise], Telefonstatus und Identität, Textnachrichten lesen, das ist jetzt ganz neu, dass man, wenn man hier diesen Facebook Messenger hat, dann werden da auch die SMS angezeigt, will ich eigentlich gar nicht, geht aber nicht mehr anders, Bilder und Videos Audio, [sie scrollt weiter durch Einstellungen von Facebook app], präziser Standort, Kontakte, email, [sie scrollt weiter und liest], die haben echt alles ne [sie lacht hysterisch].*

Ralf, Beate, Ute, Saskia, Berthold, Jörg, Heike, and Elke have never read the privacy policy of their favorite app, with Ralf admitting:

> I mean, probably in help, well, so far. I mean, one does not read it, you click "accept" and that's that.
>
> *Also ich meine, das kann ja auch kein, wahrscheinlich unter Hilfe na bisher, sowas liest man auch nicht durch, man macht ja den Hacken und das ist gut ne.*

Florian and Wolfgang supposedly read the privacy policy at one point. Wolfgang has his favorite app linked with his Facebook account: "... but I really did, it was the first time that I did, that I read through everything." *("aber da habe ich mir halt, da war es das erste Mal, dass ich das so gemacht habe halt, tatsächlich alles durchgelesen.")*

Finding the privacy policy for their favorite app proves to be complicated and not straightforward for Ralf, Beate Florian, Saskia, Berthold, and Heike. Berthold searches:

> … Well, directly here, I don't find any privacy policy. Hmm, maybe if I look into the app directly [goes back to the app] … okay, that's the settings [looks into app], to read them we have to go to the website of the app developer.
>
> *... Also, hier direkt ist jetzt noch nichts zu den Datenschutzrichtlinien, vielleicht ist es auch doch noch selbst in der App zu finden [geht auf die App zurück], aber das sind ja entsprechende Einstellungen [er schaut auf die App], also, um das nachzulesen, müssen wir dann schon auf die Webseite gehen von Entwickler.*

Two students said that they did not have to read the privacy policy of their favorite app since the apps had been either recommended by a coworker (Florian) or recommended by an unidentified source (Beate). In Elke's case, she reviewed the app's website.

7.3.5.4.2 American Students

Half of the American students (Marsha, Ryan, Liam, Abigail, Jack) do not know what personal information their favorite app can access.

Ryan confesses, "I cannot say that I do. I don't know that I ever thought about it; I have been using it for so long, that I never even considered that it is probably collecting information."

Abigail goes to Instagram:

> Ok, so I go into the settings [she goes to Instagram on her app and then goes to options] see Instagram options and make it into a private account, other things like the blocked users, other people looking at your account just in case of safety or whatever, the two-factor authentication, which is I think a great idea — people could easily find your password or whatever, so it is a great way to ensure there are more steps.

Ryan, Owen, and Ava have to search for a while before they find the privacy policy of their favorite app.

Ava states:

> Hmm, I wouldn't know exactly where it is. I mean, I just checked under settings [she is looking for it on the app now] — no that is not right; I would probably search for it, if I looking for it, or I would google IFTTT privacy [she picks up phone and does that], or I would go to the privacy settings on my phone and look it up.

All the other students find the privacy policy relatively quickly. Marsha reads through Whole Foods app's privacy policy again:

> Personal information, ahem, I don't think I gave any – don't give any of this information – that is the thing I don't remember, because you cannot buy things through the app. So, it is not that I put in a credit card, so I don't know, they have it probably in case they want to expand, but you put in your name and your email address [she goes back to policy and scrolls some more] so they can get IP address, browser, device, hardware type, operating system, data regarding network connected, hardware click stream data, logs.

Nevertheless, none of the students have ever read the privacy policy of their favorite app. Luke, who never read it for Spotify, admits, "I am not too sure about that. I didn't look into it," and Liam's response about Twitter is similar:

> I actually never have. I, again, being an IT major, I know that Facebook sneakily updates its privacy setting even though you have agreed to previous ones, they put in things … I don't know if you can get it here [he means the app], I just don't know, you probably could, I just don't know. Yeah, so.

7.3.5.5 Privacy Policy Attitude

Many apps include a privacy policy in the Apple App/Google Play stores. Various apps also include their privacy policy in the app itself. None of the study participants tried to look for or read through the privacy policy in the experiment part A. Moreover, only a handful of students have ever read through the privacy policy of their favorite app. In the next sections students' attitudes to privacy policies will be described.

7.3.5.5.1 German Students

Ralf, Beate, and Wolfgang's reasons for not reviewing or reading privacy policies are that they are too long and written with legal terminologies that make them difficult to comprehend.

Beate openly questions, "and do you understand it? *("und versteht man es?")*

Ralf admits that he doesn't want to waste his time:

> No, it is too long to read; I don't understand it, it is written in legalese, I don't know, I don't care, I don't want to waste my time.
>
> *Nö, das ist einfach zu viel Text, den ich nicht verstehe zum Teil, und halt auch ist einfach so Juristendeutsch, keine Ahnung, das interessiert mich, also da will ich keine Zeit verschwenden.*

Wolfgang believes that many privacy policies "talk more about their philosophy instead of what they are actually doing." *("... und die reden da halt viel zu viel über Philosophien eigentlich und nicht darüber was sie tatsächlich machen.")* Furthermore, he thinks that if they are really long, it is possible to hide essential facts.

> …If someone wants to harm me and they want to protect themselves legally, well then, they could write harmful/nasty things into the wrong paragraphs, hoping that I don't read it.
>
> *..., Wenn jemand mir wirklich was Böses will und sich rechtlich absichern möchte, dann schreibt er halt im Kapitel, wo es eigentlich nicht richtig reinpasst halt, die schlimmen Sachen rein, in der Hoffnung, dass ich es dann nicht lese.*

Spotify was one of the first apps that Wolfgang connected to his Facebook account. He went through the hassle of reading the privacy policy:

> To make sure, well, sort of to avoid the danger of some company being able to read and use my personal information and data from Facebook.
>
> *Um nicht, um quasi der Gefahr zu entgehen, dass da jetzt irgendein Anbieter meine Facebook Daten halt einfach einsehen und irgendwie nutzen kann.*

Berthold acknowledges that it takes him a while to find the privacy policy for his favorite app and then remarks:

> Well, I think they explained the most critical aspects of the app already; in the description of it in the app store, and on the support website FAQ. I feel you don't actually need to read the privacy policy.
>
> *... Haben sie ja alles Wesentliche zu der App eigentlich schon recht gut erklärt, also sowohl jetzt im App-Store in der Beschreibung als auch auf der Supportwebsite mit FAQ. Ich finde man erfährt dann auch alles Wesentliche, ohne dass man jetzt konkret die privacy policy [sic] nachliest.*

Trusting a coworker's recommendation or the company's website is why Florian and Elke do not think it's necessary to read the privacy policy of their favorite app (Threema). Elke declares:

> To be honest, before I installed it, I looked at the website [of the app] and decided to install it. So, I went there, but then not within the app itself.
>
> *Ne, ehrlich gesagt habe ich das schon, bevor ich das installiert habe, schon mir vorher auf deren Webseite mir angeguckt und, da habe ich deswegen mich dafür entschieden, das zu installieren, also war schon, aber in der App dann nicht mehr.")*

7.3.5.5.2 American Students

American students also think that privacy policies are "too long" (Marsha, Ryan, Owen, Abigail, Luke, Jack, Steve).

Marsha declares:

> They are long, ahem, *long*. Like, I had to do the like the IRB[39] training thing and they were talking about making your information like the thing that I have to sign, making it like clear and understandable, tailored to whomever your audience is. I think it is like, first off, [the] text style is, like super-small, no one is going to sit there and read it, there is no images, it is not clear, there are super-long and they also repeat it. [But] I also don't want to exclude myself from things. I don't want to sit there and [wonder] like, "Is it ethical on their part?" I don't know?

Ryan echoes this perception as "[…] right of the bat, there is just too much of it. No person is going to take the time to go through every piece of it, [read] all the way through and see what the different options are."

[39] https://www.hhs.gov/ohrp/regulations-and-policy/requests-for-comments/guidance-for-institutions-and-irbs/index.html

Steve openly confesses to never reading privacy policies: "neither me nor anybody else ever looks into that. Like, people can lie but we know the truth."

Moreover, privacy policies are purposefully written in a complex manner, which he finds frustrating. Steve also assumes that as one reads the privacy policy "you will eventually not notice the little contradiction in there that basically tell you that you are giving YouTube all the rights to look at your data usage." He believes that privacy policies may include "little legal loophole "things" so that you cannot sue the app maker.

Liam confesses that he does not want to read them, and Luke does not perceive it a necessity: "I guess for me it fits. I know enough, I feel I don't really need to think too hard."

Marsha points out that she never realized they were included in the app store "down there."

Harper is the only student who does:

> Yeah, I always try. I read like the first paragraph and skim all the way to the bottom and I read like the last two paragraphs [she is smiling and laughing a bit]. […] Because I feel like I should read them, just because I am signing a legal document technically. Even so, they just disguising it at me just press accept, that is still me technically signing like a legal document, I have always been told that you need to read them.

Furthermore, Marsha does not "typically think they try to deceive people with the length. I know they probably do sometimes; they probably get away with a lot of things." However, later on she contradicts herself when she states, "I *think* they are too long, which is why I do not read them."

Three students (Marsha, Harper, Luke) have suggestions as to how privacy policies can be improved.[40]

According to Luke:

> The companies, I feel like they should also, like … things like privacy policy, I feel like they should be more noticed. It is, like, hidden; [it] should be more emphasized I guess, because I feel like a lot of people disregard looking at privacy policy. For example, I didn't look at it.

Marsha says that instead of a written privacy policy they should be all infomercials, and Harper would like it if "they could just link it on the app [she means the rating from the privacy grade

[40] These suggestions were made during the interview debriefing session.

website]. They can just say, privacy grade, when like Internet Movie Database[41] (IMDb) connects you to Rotten Tomatoes[42]. It could be kind of like that for the app store."

7.3.5.6 Personal Information and Data – Attitude

It is no secret that apps share a variety of personal information and data, but "most users of smartphone apps remain unaware of what data about them is being collected, by whom, and how these data are being used. "(Van Kleek et al. 2017). This subchapter describes participants' thoughts on personal information and data sharing related to smartphones and apps.

7.3.5.6.1 German Students

German students (Ralf, Beate, Wolfgang, Ute, Florian) assume that the personal information and data being shared from their phone includes at least mobile phone number, email address, contact lists, browser search history, and age.

Ralf assumes:

> Yeah, in any case, where I live, probably, age, and personal data. Mobility pattern I would say, and what I Google and where I am when I Google something. Maybe connections between things, who I know, who is in my contacts.
>
> *Naja, auf jeden Fall Wohnort wahrscheinlich, Alter und persönliche Daten, Bewegungsmuster sage ich mal, auch, was google ich oder wo bin ich, wenn ich was google, vielleicht Verknüpfungen herstellen und solche Geschichten, wen kenne ich, wen habe ich in meinen Kontakten.*

Beate assumes her shared data include "probably my log files, if I use apps, what I am looking at, how I am looking at it or how long and such things ..." *("wahrscheinlich auch meine log files [sic] gerade, wenn ich Apps benutze, was ich mir angucke, wie ich es mir angucke, wie lange oder sowas, kann ich mir vorstellen, auf alle Fälle gespeichert wird.")*

Referring to his browser history, Wolfgang says:

> … Ahem, so much information can be derived from what pages I look at. Theoretically, there is a lot more information behind it, more than anything else, well, and I don't know, I mean theoretically each text message I write includes data that could be collected and analyzed.

[41] https://www.imdb.com/

[42] https://www.rottentomatoes.com/

... Ähm, kann da halt unglaublich viel daraus gezogen werden, was für Seiten ich mir angucke, das steckt einfach noch viel mehr Informationen theoretisch drinnen, als im allen anderen irgendwie und ja ich weiß nicht, meine rein theoretisch wird jede Textnachricht, die schreibe, sind halt Daten, die in irgendeiner Weise gesammelt und ausgewertet werden können.

For Florian:

> Usage statistics, usage length, search terms, what I enter — but I am assuming that all apps are doing it, not all apps are collecting, but it is a potential source of data, it is really interesting – what the user searches for.
>
> *Nutzungsstatistiken, Dauer, es können Suchbegriffe sein, Eingaben, aber das ist, würde ich nicht unterstellen, dass das in allen Apps gemacht wird, alle Apps darauf ausgelegt sind, das abzugreifen, aber es ist eine potentielle Quelle an Daten, die wirklich sehr interessant sind, was sucht der Nutzer.*

Several students (Ute, Florian, Berthold, Elke) mention that their personal data and information is being shared primarily with Google, because as Ute says, "well, Google is omnipresent on Android." *("naja Google ist ja immer omnipräsent mit Android.")* Facebook, WhatsApp, Amazon, and app and advertising companies are also mentioned.

Saskia assumes that these companies also sell personal user data to each other:

> Well, I imagine it like this: they sell it all to each other — Facebook, WhatsApp …, not sure, maybe Amazon, Amazon for sure.
>
> *Also, ich stelle mir das so vor, dass die vielleicht alles so untereinander verkaufen, also Facebook, WhatsApp (...) weiß ich nicht, vielleicht auch Amazon, bestimmt Amazon.*

Ralf calls them:

> Data collectors, those are, sorta … I imagine it's like it used to be with telephone numbers being sold, with phone numbers of real people. I assume it is the same.
>
> *Datensammler die, also ich stelle mir es so vor, wie Telefonlisten, die verkauft wurden früher, also Telefonnummer von echten Leuten, wird wahrscheinlich so genauso sein.*

Beate imagines:

> That insurance [companies] would like to obtain my fitness data illegally. I mean, I can somewhat understand it. I mean, looking at it from their point of view, [I understand why] they would like [to have] it, maybe even my cooking recipes because then they could figure out what I eat.
>
> *Ich kann mir vorstellen, auf den den [sic] illegalen Weg Versicherungen würden bestimmt gerne Fitness Daten haben, kann man nachvollziehen von deren Standpunkt aus, das die gerne die Daten haben wollen, vielleicht sogar am Ende meine Rezeptdaten, weil die in meine Ernährung reingucken können.*

Wolfgang is the only student who cites his cell phone provider as having access to his personal data:

> Well, theoretically of course, my cell phone provider, I mean it has to be like that so that everything works. But it is a bit creepy if I set up my cell phone, I receive a text message from my mobile phone provider, and my phone is being set up without me being involved at all.
>
> *Also theoretisch mein Mobilfunkanbieter natürlich, der sowieso, das ist so, ich meine, muss ja auch, damit das alles funktioniert, aber es ist halt so ein bisschen unheimlich halt, wenn ich das Handy halt neu einrichte, dass ich dann von meinem Anbieter eine SMS geschickt bekomme, die dann von meinem Telefon automatisch, ohne dass ich was tue, interpretiert wird.*

Half of the German students (Ute Florian, Berthold, Heike, Elke) believe that governments, the secret service, or even the NSA have access to their personal information.

> Yes, and the NSA and the like, I believe that the the [sic] NSA, knows quite a lot about what we are doing on our devices.
>
> *Ja, NSA und so, also, glaube ich schon, dass die die NSA nach wie vor über ziemlich viel im Bilde/im Bilde sind, was wir so auf unseren Geräten machen.* (Ute)

According to Berthold:

> Well, principally, the question is whether the NSA or some other governmental entities or secret services are interested in the data or if they [need to] have some evidence [in order to] be allowed to collect my personal information, or if they just collect the data to have it in stock [we both are laughing].
>
> *Ja, ansonsten hätte man sonst noch prinzipiell die Frage, ob sich die NSA oder sonst irgendwelche Behörden oder Geheimdienste ja nicht nur für die Daten interessieren oder ob sie irgendwann Anhaltspunkte haben, sich mit einem persönlich zu beschäftigen, oder ob sie nur generell alles sammeln auf Vorrat [wir beide lachen].")*

Some students (Ralf, Jörg, Beate, Heike) openly admit their own difficulties in understanding what kind of companies have access to their personal information and data: "I don't know. If I am honest, it is hard for me to assess." *("Das weiß ich nicht, kann ich überhaupt nicht einschätzen, wenn ich ehrlich bin. ")* (Ralf).

Supplementing this, Jörg states:

> That's a good question: Who has access to what? I'm just not sure, it is a big gray area, which I think is problematic. Personally, as a user, I feel I do not know what's going on in the background. I do not know which parts of my personal data are being shared and which are not.

> *Das ist eine gute Frage, wer auf was Zugriff hat, da bin ich mir eben nicht so ganz sicher, diese große Grauzone, das finde ich auch gerade so dieses Bedenkliche. Ich persönlich habe als Benutzer das Gefühl, ich weiß gar nicht mehr, was im Hintergrund alles stattfindet. Ich weiß nicht, welche Daten von mir rausgehen oder was nicht.")*

And Beate views it as "this is the problem between transparency and not understanding what is possible." *("Das ist halt schon, das ist halt das Problem zwischen Transparenz und nicht wissen, was geht.")*

All students point to advertising and commercial profits as one of the main reasons why companies seek to access their personal data.

Ralf says:

> I mean advertising [he is laughing] … personalized advertising, but maybe also to figure out *how* to sell stuff better. The purpose is to make money.
>
> *also, ich Werbung [er lacht] (...), glaube ich, spezifische Werbung schalten vielleicht, aber auch einfach rausfinden, wie man Sachen besser verkaufen kann, also, ich glaube, da sind einfach viel kommerziellen Absichten."*

Berthold declares, "Google is the biggest advertising agency." *("Google an sich ist natürlich auch das größte von allen Werbeunternehmen.)*

Elke admits:

> Well, I don't know all the reasons, but mostly to make a profit by selling data to advertising companies so that they can create personalized advertising. But the worst-case scenario is to influence political opinions.
>
> *Also ich kenne natürlich nicht alle Interessen, aber die geläufigste ist, um daraus Geld zu machen, indem man die Daten verkauft, an Werbungsunternehmen, die dann personenbezogen Werbung entweder oder im schlimmsten Fall politische Beeinflussung."*

Ute, Wolfgang, and Heike perceived personalized advertising as advantageous to them.

Ute appreciates it "when one searches for products, that is online shopping, one gets a recommendation for a personalized product." *("auch, wenn man nach Produkten also online Shopping macht, dass man dann halt passende Produkte dann vorgeschlagen haben will.")*

And Heike says:

> Amazon, if they know your purchase history, they offer me things that I might actually like, things like that (...) It can be perceived as beneficial for customers.

Bei Amazon, wenn die schon wissen, was du vorher gekauft hast, dann bieten die dir halt Sachen an, die dir halt auch gefallen könnten, und sowas und (...) für den Endverbraucher kann man das als positiv sehen oder ...

Many students perceive personal information collection and sharing as a "trade" for free apps and services, and that is quid pro quo. According to Ralf, it is "somewhat [of a] balancing act to get something for free; it is a conscious trade." *("das ist ja immer, so ein Abwägen von Ich-will-was-für-umsonst-haben, ich finde, das geht man ja bewusst ein, den trade [sic], sage ich.")*

Beate echoes this by saying:

> So, I think you just have to be aware, you just cannot ask for some things if you're not ready to give something in return [...] without the user data, Google would not be so effective, and it is convenient. That's the question then, whether it is worth for me, that's the question I always ask myself, "Is it worth it to me to give away my information for what I receive in return?"
>
> *Also, ich glaube, man muss halt sich klar sein, man kann halt manche Dinge nicht verlangen, wenn man nicht bereit ist, was zu geben […] Google wäre nicht so gut, wenn sie nicht Daten hätten und Bequemlichkeit, die man daraus gewinnt, ist halt die Frage, ob es das einem Wert ist, das ist die Frage, die ich mir immer stelle, ist es mir das wert, die Daten, die ich da hergebe, für die, für das plus dass ich quasi damit mache.*

Wolfgang knows that in return for a free app he must pay some sort of price:

> Well, if I buy something, I mean if I download something for free, they can get my data. If not, it would be [getting] something without paying for it.
>
> *Derjenige, von dem ich was kaufe, bekommt auch meine Daten, also, wenn ich mir was Kostenloses runterlade, ist das ja trotzdem, wie Kaufen für kein Geld.*

Ute and Wolfgang do not mind sharing personal information in some cases.

> Yes, so when it comes to self-improvement, it's always okay, because otherwise, it does not work because no one fills out any feedback surveys, so if they want to get better then they have to [do the] research themselves.
>
> *Ja, also, wenn es um Selbstverbesserung geht, dann ist das es immer okay, weil anders funktioniert die nicht, weil keiner füllt irgendwelche Feedback Befragungen aus, deswegen, wenn die besser werden will, dann muss die sich selbst erforschen.* (Wolfgang)

And Ute states:

> If I use Android, then Google knows everything, but I do get something in return. So, if [Google] uses it to improve their service, well then, I get something out of it, too.

Wenn ich jetzt weiß, ich benutze Android, dann weiß ich, gebe alles an Google preis, aber ich kriege ja auch was dafür, also ich, wenn die [Google] es nur für sich selbst benutzen als Selbstverbesserung, dann hat man ja auch was dafür.

7.3.5.6.2 American Students

Ryan, Owen, Liam, Harper, Abigail, and Ava identify the types of personal information and data they believe is accessed via their smartphones.

Ryan says:

> (...) My hope [laughing a bit in a nervous way], in the best-case scenario, [is] that the only things being looked at are, like, things like browsing history and patterns of maybe, maybe shopping: if I am going on Amazon or something like that, [what] products that I am looking at. I know that a lot of sites now have cookies and trackers that can kind of see where/what parts of an article you looking at, whether you scroll through the whole thing, or whether you looking only at parts of it. How quickly you looking at articles, which can give them a pretty good sense of how much of an article you are reading versus if you are skimming through it or if you are just reading the headlines.

Steve proclaims:

> I am not exactly a fan of like big data and its usage, but it is pretty much the responsibility of user to see this pattern to understand that it is happening, I believe anything like these companies are like to me should make it clear that this is happening and if you don't want it to happen you are going to have to make some changes to your lifestyle on the phone or on the internet.

Liam believes that most app companies have access to his information and contacts:

> One app connects to Facebook and [when you] put your birthday on Facebook that means they have access to it now, too — so it is like a chain reaction to whatever you download. You put out information and then … yes, and the next app and the next app …

Jack expects companies to share his data with other companies: "I think Snapchat … they probably give it to other people and companies … Instagram definitely does it, Facebook does it."

Ava assumes that:

> Google collects information on your browsing history — even if I did not know that specifically, I can see it happen [laughing]. Like, you know, you check out something on one app and then you go on Expedia and all of a sudden Facebook is advertising Expedia stuff to me.

All students consider Google to be the most prominent company tracking their personal information and data. "Google has access to all my information — like I said earlier, I literally live on Google. Google Cloud, they have access to all of my information. Hmm …" (Harper). Marsha feels like:

> Google has everything already anyways … No matter where you are, they just, they already know. I think that is also surveillance; I feel like a lot of it is already known or has been shared, kind of what is the point at this point? Like, we were kind of thrust into it like being of the generation that didn't quite grow up with it, but got it early when we were kids. We were just given it, so we just did stuff with it, so we now it is like – I am sorry, it is already all out there.

Luke believes "big data companies, like Facebook, Google, so Facebook actually know a lot … and Amazon. Are there some others? I am pretty sure there are lot more, but usually, those are the big ones."

Facebook, Instagram, and Apple are referenced by many other students, too. Abigail feels:

> A lot of social media does have content. Say, if I am on Amazon, like looking at a product like the Fitbit or whatever, it shows up on my Facebook feed." Liam says, "I don't know, but any company Apple works with, really. I guess that is like the general thing.

Only Steve brings up his cell phone provider and only one student (Ryan) mentions the NSA, as he declares:

> Well, I have the Dropbox app installed on my phone, but if I was on my phone, but if I am talking about that service then technically I know they have access to my data. So, I know the NSA, I am pretty sure they [Dropbox] are in the PRISM program, so they have access to my data …

The primary motive for companies collecting data is, according to all students, advertising and making a profit. Ryan asserts:

> By collecting that information, they able to build a profile that they can then sell to marketing companies that are looking for certain kinds of consumers so that they more likely to get money off me, basically, if they send me advertisements or target[ed] messages.

Moreover, Liam proclaims, "I think it is more for their gain than it is for our gain when we use an app […] *I believe it is so*." Ava assumes that:

> Most of it is just used for, for advertising, but I know sometimes if you use a shadier app or a shadier company, you might get spam email, so they probably sell your email address multiple times over, and I mean it is basically like a money-making thing. They

> just want you to look at more stuff and beyond the apps more: the more you click on certain things, the more money it generates, so I think that is mostly what it is used for.

Several students are also in favor of personalized ads. As Ava declares:

> So, I don't mind [personalized ads] if it is advertising things I might be interested in. I am more likely, if I keep seeing an advertisement … if I see it on Facebook, if I see it on another app, if keep seeing the same kind of advertisement I am more likely to click on it and see what it is about, and I [have] found some really cool apps that way.

Jack's attitude is similar: "like their customizing, you know how you get those ads on Facebook, that are customized just for you? I like would rather have an ad customized for me than an ad customized for you. We have different taste[s]."

The improvement of apps, services, and technologies is another reason for not being bothered by data collection. As Harper explains:

> I don't think they obviously target individuals; I think they use it for a lot of research like customer research. I think they definitely use it in order to improve the app [performance] but I also do think there are people who could sell that information, obviously illegally. I don't know [who] those people would sell it to or what those people would do with this information, but I obviously know it is there. I like to believe they are just doing research and stuff with it; that is obviously not always true — like I said earlier, I feel they do make some sort of personal profile of you and then they use it in order to target advertisements and searches toward you … I know Facebook does that a lot and it is really creepy [that] I can look up something on Google and then Facebook will know somehow and give me the advertisement, which is creepy, but …

Luke assumes that they use it to analyze his data, but then he points out that:

> ... You never really know if they are actually doing something dark or anything, they could be … like, invading your privacy. They are using it for the betterment for themselves and not so much, the, basically they don't consider, like, the other people, so they use it for their own benefit just to gain profits or something like that. But they usually use it for like predictive analytics; yes, they try to predict consumer behavior, like they try to find the best way in order to serve them better, so it is all about analyzing data. Like, Facebook, they probably do like some kind of emotional trend [analysis], because they are basically an information provider, so they are not necessarily just a social networking website. So, like, they just try to track to see how people, yeah like how information, like how the news actually affects people. Sometimes they can even alter someone's newsfeed to [make them feel] more happy [sic], that can actually affect if the person becomes happier, so they can manipulate certain data and like that.

Owen considers it a fair trade:

> If, let's say, a user blocks all their information, but they can still use all the Google services, then Google is just giving them [a] free service. They have free photo storage, but Google cannot sell their algorithms to [make improvements]. In Google's eyes, that person is just like a freeloader, they just using their services for nothing.

Ryan is cognizant of the fact that "when a product is free, *you* are the product, and they are gathering information on you because that's how they make their money."

Abigail is somewhat conflicted, because when:

> You are using their product, they are going to *see* the people using their product and when you post something on their sites, it is being posted in their coding. They see the coding, they see the whole backend of everything, so to me it is kind of weird how people that I don't know can see this. But at the same time, I am a consumer, I am using their stuff, [and] I can see *why* they'll see it, because it is for their own data and for their own information for the company.

Jack is the only student openly in favor of companies using his personal information:

> I don't mind these companies collecting my data because they just trying to, like, gather data from everybody [in order to] to compile it and use [it] for future ventures. So, I don't mind that they [perform] data analysis, and I think it is a good thing they do that. […] It helps them out; it helps them to be bigger and better.

Some students are confused about how, if, and in what way their personal data and information are shared. As Marsha wonders:[43]

> [she goes onto her phone into privacy settings] This was weird to me, the advertising thing [the limit ad tracking option under the privacy option for the iPhone] … Because it seemed unclear … Umm, I am, like, if I turn that off, [do] I get more ads, [do] I get the same number of ads, but less relevant [ads to me] if it is on, or am I opting out of it right now and I get less relevant things, it is weird.

Also, according to Ryan, if:

> Corporations are mostly holding the information, it is not open to the public … I would very much like to know, what is the information that is being gathered about me, what are the actual pieces of data that you have about me, who is gathering it? Which can be really hard [to] [figure] out in the first place.

[43] She made this comment during the debriefing section of the interview.

7.3.5.7 The Transparent Human *(Der gläserne Mensch)* – Attitude

The German phrase "*gläserner Mensch"* (transparent human) is used as a metaphor for data privacy. Here is a good definition from Heizereder (2015):

> Which websites you go to, what you shop for online, who you email or text, who you are talking to on the phone, where you are right now, what you like and what you do not like — an unbelievable amount of your data is floating around. You are on the right track to becoming a transparent human.
>
> *Welche Internetseiten Sie aufrufen, was Sie online einkaufen, wem Sie Emails oder SMS schreiben, mit wem Sie telefonieren, wo Sie sich gerade befinden, was Ihnen gefällt und was Sie gar nicht mögen. Schier unfassbare Mengen an Daten von Ihnen sind im Umlauf. Sie sind auf dem besten Weg, ein gläserner Mensch zu werden.* (Heizereder 2015, 649)

In the following subchapter the differences of attitudes and behaviors of the following question is depicted:

> What are both groups of students, the American and German students,
>
> think about being, or becoming, a transparent human *(gläserner Mensch)*?

7.3.5.7.1 German Students

Not accepting the fact that she may be "transparent", Elke states:

> In any case, well, I think it has to change. I think the term "transparent human," I am not sure if it is the best term anyway. But to say I have nothing to hide, I don't think that is ever the case.
>
> *Also ich denke, dass muss sich auf jeden Fall ändern, ich glaube auch gläserner Mensch ... weiß nicht, ob das so ein glücklicher Begriff ist, aber nichts zu verbergen zu haben, halte ich für einen absoluten niemals zutreffenden Ausdruck ...*

Elke then emphasizes her position with two arguments: First she doesn't know what essentially emerges out of the data collected, and thus it is hard to fathom. What if, retroactively, she would have preferred to keep it private? Second if she looks at it from a dystopian side, what if a democracy changes and suddenly her personal data is surveilled, perhaps because she is a political activist or she belongs to a specific political party?

Berthold agrees:

> Well, I think it should not become *too* transparent, even though I think it already is pretty transparent ... one has to find a balance for each service, each case. It is always [about maintaining some] balance between security and data privacy on one hand and,

on the other hand, to take advantage and have the convenience of getting restaurant suggestions, a restaurant that fits my personality, or if I want to protect my data privacy and thus I will not receive personalized recommendations.

Ja, ich denke schon, dass es nicht zu gläsern werden sollte, auch wenn es oft schon sehr gläsern geworden ist, … und ja, man muss einfach in jeden Anwendungsfall, von den man selbst auch profitieren möchte, abwägen. Ist ja immer dasselbe zwischen Sicherheit und Datenschutz auf der eine Seite, tja und den Komfort und den Möglichkeiten, die die Nutzung dann bietet, den Vorteilen, ob man jetzt das so nützlich findet, dass einem das nächste Restaurant vorgeschlagen wird, das einem auch gut gefällt auf jeden Fall oder, ob man lieber seine Daten schützt, und niemand so tolle nützliche Vorschläge einen bringen kann.

Ralf finds it acceptable if other people share all their personal information, but he personally does not see the benefit:

Yeah, because if you become transparent, you expose yourself. I personally don't see the benefit of it, to be honest; I find it somewhat … stupid to be made into a transparent human.

Weil ich mein, also dieser gläserne [Mensch], also ich finde, dass man sich da halt sehr viel exponiert, ohne davon, also ich selber ziehe da keinen Mehrwert draus … ich finde das eigentlich ... doof, dass man so durschaubar gemacht wird.

Two students, Heike and Wolfgang, hesitate; on one hand, they talk about the advantages of data transparency:

From the technical side, and to consider efficiency, the transparent human [idea] is appealing, it offers massive potential to improve life, one could automate many things. Well, I don't know, I am thinking about stocking my fridge with food that I want to eat next week …

Hat das auf einer rein technischen und irgendwie Effizienz-Ebenen hat der gläserne Mensch an sich einen riesigen Reiz, weil es halt riesigen Potential dazu hat, unser Leben unglaublich zu verbessern … ließen sich einfach dann auch eine Menge Sachen dann auch automatisieren, also, weiß ich nicht, ich denke da halt an Kühlschränke, die automatisch die Sachen kaufen, auf die ich nächste Woche Lust habe. (Wolfgang).

Heike stresses the benefits of personalized advertising:

Well, first and foremost, I find the term "transparent human" a bit scary because …right now, the development — and I am not talking about smartphones only; for example, your shoes have a tracking device, as does your car and everything else — means someone could follow my entire life, when ultimately it is nobody's business.

Ja, also in erste Linie finde ich erstmal der Begriff "der gläserne Mensch" erfühlt mich erstmal mit Unbehagen, weil ... weil im Moment entwickelt sich das alles in so eine Richtung, wo man also, das geht ja nicht nur über das Handy, dann hast du an deinen neuen Schuhen noch so ein tracker Dingsbums dran und im Auto und überall, könnte

man dann dein ganzes Leben nachzeichnen, und ich finde schlussendlich geht das eigentlich keinen was an.

Wolfgang goes a step further, because he thinks that humankind is not ready to make this leap:

> I don't trust humankind, or the companies in charge of ensuring [data transparency] works efficiently, having to gather all data from different sources for each existing person. That is eerie, because then there is one entity with all the power. Because they have all the data, it has to be centrally administered.
>
> *Ich traue der Menschheit einfach nicht genug dafür, also, die die Firmen, die sich darum kümmern, damit sowas halt richtig richtig effizient funktioniert, müsste man aus vielen verschiedenen Quellen, alle Daten über jede einzelnen Person, halt zusammentragen, die es eben gibt. Das ist eben dann komisch, weil es dann irgendwo eine Instanz gibt, die halt eine zu große Macht Position hat, weil sie all diese Daten, das muss zentral verwaltet werden.*

Two students (Heike and Saskia) are, in theory, not okay with all of their personal data and information being out in the open and available to companies. Saskia believes that most people would agree with her:

> I don't know, a cell phone is more personal compared to a computer or laptop, because one always carries a cell phone, and as soon as you know what's on a cell phone, you know everything or a lot about a person: how they behave, and of course that is not okay ... well, theoretically, it is not okay, but practically you are supporting it because you are still using these apps ...
>
> *Ich weiß nicht, weil das Handy noch einmal eine Nummer persönlicher ist wie ein PC oder ein Laptop, weil das Handy eigentlich immer dabei ist und sobald du weißt, was alles auf dem Handy ist, weißt du eigentlich alles oder vieles über den Menschen, was er tut, wie er sich verhält, und das ist eigentlich natürlich nicht okay … also in der Theorie ist es nicht okay, aber in der Praxis unterstützt man es ja, weil man ja trotzdem die Apps hat.")*

Heike concurs that "in real life one doesn't care too much." *("aber in der Praxis macht man meistens doch nicht soviel dagegen.")*

Beate believes sharing personal data has legitimate uses as long she has been informed about it.

> I think it is okay if I know about it: then I can make an informed decision; but it is not so great if I have not been asked, and people use it to manipulate you ... I am thinking about advertising; it is an uncomfortable feeling to know, "Well, they know this about me, not because I gave it to them, but because they bought it somewhere."
>
> *Dann finde ich es okay, weil dann ist es ja auch, dann macht man das bewusst die Entscheidung, schlimmer finde ich es, wenn man gar nicht erst gefragt wird und es*

einfach gemacht wird und Leute das auch benutzen, quasi um dich in wirklich in eine Art zu manipulieren … da denke ich viel an Werbung zum Beispiel, das ist einfach ein ungutes Gefühl, dass man hat, wenn man halt merkt, okay die wissen das über mich, aber nicht, weil ich es ihnen gegeben habe, sondern die haben sich es irgendwo gekauft.

Ute does not view herself as a "transparent human", but she expects it and favors data personalization. She also proclaims:

> Inasmuch as I don't think that any information that I don't want to be *somewhere* is somewhere [laughing] ... and I think that I somewhat know what data I've released, and I am okay with it, and therefore ... [she shrugs]
>
> *Insofern ... insofern, dass ich nicht denke, dass irgendwelche Informationen, von denen ich nicht will, dass sie irgendwo sind, irgendwo sind [lacht] ... und ich denke schon, dass ich ungefähr weiß, ich, welche Daten ich preisgebe, und dass ich, mit denen auch einverstanden bin, und deswegen… [zuckt mit den Schultern].*

Jörg offers a different take:

> So, for me, it is social development. It used to be that, back in the '90s, computers were still [available to] a [select] few people ... today, everyone owns a smartphone ... everyone uses it all the time, and that's why, for me, data protection and privacy is not only a technical question but also a question of society and societal norms ... However, at the moment, I consider it "normal" how we, as humans, have to learn not to make ourselves too transparent.
>
> *Also für mich ist das auch so, das ist eine soziale Entwicklung, vorher war das wirklich so, damals noch in den 90er Jahren, waren Computer noch wenigen Menschen vorbehalten, … heute besitzt jeder ein Smartphone, … jeder benutzt sie permanent und deswegen ist das für mich mit dem Datenschutz und der Privatsphäre auch nicht immer nur eine technische Frage, sondern auch eine Frage der Gesellschaft und der Sozialform …, aber an der Stelle betrachte ich es eben als soziale Form, dass wir Menschen persönlich auch lernen zu müssen, uns nicht gläsern zu machen.*

A few students remark on how stricter laws, increased regulation, and support for open-source software could foster mobile privacy for consumers.

As Ralf states:

> Or to be more rigorous, the problem is, even if I don't share information, other people using Facebook and WhatsApp share information about you, and often you cannot control that. And because of that, the law has to forbid it, probably.
>
> *Oder halt wirklich rigoros, ja das Problem ist auch wie gesagt, dass du selbst, wenn du selber keine Informationen teilst, halt Leute die halt so ne Sachen benutzen wie Facebook oder WhatsApp, halt trotzdem halt Informationen über dich halt teilen, und das ist halt, das liegt halt nicht unbedingt in deiner Hand und deswegen müsste man halt einfach sagen, das gesetzlich verbieten wahrscheinlich.*

Florian would like big tech companies to have less power. He is in favor of more support for mobile open-source software.

> The market power that they have, it is enormous, and I would not mind if it was fundamentally cut ... I could imagine, for example, subsidies for free operating systems, *real* free operating systems.
>
> *Diese Marktmacht, die man sich erobert hat, ist schon enorm und ich hätte nichts dagegen, wenn die grundsätzlich beschnitten wird ... Ich könnte mir zum Beispiel Förderungen für freien Betriebssysteme, also richtig freie Betriebssysteme vorstellen.*

Wolfgang trusts neither the government nor private companies to manage and administrate humankind's personal information and data, suggesting:

> Well, the only ones I would trust would be the Jedi but they do not exist, that's why we cannot do that ... Yes, but that's the only fictional entity I trust to have the wisdom to manage it responsibly.
>
> *Also die Einzigen, denen ich das zutrauen würde, wären die Jedi, aber die gibt es nicht in Wirklichkeit, deswegen können wir das nicht machen ... ja, aber genau die sind einzige fiktionale Entität, die ich kenne, die die Weisheit besitzt, um so was verantwortungsvoll zu verwalten.*

Beate, Jörg, and Heike think that awareness and education on mobile privacy issues need to improve.

> I think is important that there is education, not only led by consumer protection agencies, but also by schools.
>
> *Und sowas finde ich dann halt schon wichtig, dass man da aufklärt für genug, jetzt nicht nur vom Verbraucherschutz, sondern auch von der Schule aus.* (Beate).

For Jörg, it is:

> Why, I think, the awareness of what one does has to be raised, people have to be made aware … because a lot of personal information is still ours, and that's why the awareness needs to be there.
>
> *Also deswegen denke ich gerade, dass auch dieses Bewusstsein, was man eigentlich tut, das muss gestärkt werden, das muss den Leuten wirklich bewusst gemacht werden … aber viele private Informationen liegen doch an der Stelle noch in unserer Hand, deswegen denke muss da gerade mehr ein Bewusstsein einsetzen.")*

7.3.5.7.2 American Students

Marsha, Liam, Harper, Luke, Jack show signs of indifference when it comes to being "data transparent."

For example, Marsha confesses:

> I think there is a level of complacency, hmm … Not that I am totally okay with it, but it is just, like, I feel like it is kind of "how it is," umm, and I could go back to the "Note to Self" [podcast] emails — I should do that, I should do that — but it is, like, I am kind of … yeah, it is already out there.

Liam agrees:

> I mean, when you think about it that way, I guess it is scary in a way because anyone that can get through to their servers or their systems can have access to you. But at the same time, for example, Twitter and Instagram, they are for entertainment [purposes], and they [improve] your quality of life better, so, for the most part, I access it. You kind of disregard that, put it on the back burner, kind of concentrate on what entertainment they provide to you and, yeah.

Luke, Steve and Harper somewhat accede to data and personal information transparency.

> Umm, am I actually okay with it? No. Do I feel like I need it, [that] I need to not to worry about it in order to survive in this kind of environment that we live in? That is a different question [she is laughing] … and I don't like [it] but I don't think I have a choice anymore as to whether not I can like it or not, which is terrifying but at the same time … (Harper).

Luke shares a similar viewpoint:

> I guess it is the norm … and we cannot really do anything about … so, I guess I have to accept it, I cannot really have it any other way … Because in order to do what you want to usually do, I feel like some data has to be transparent, yeah; if you really want to get off the grid, you probably need to live in the jungle.

And Steve states:

> It is a technical monopoly but it is not a *monopoly* monopoly like J. D. Rockefeller and that type of thing … We are living in an age where privacy is a rare thing ... so far Big Brother hasn't rolled in the squads yet. Well, it is a good think to keep in the back of your mind to not let the government go too far, there is a reason why that book [*1984*] was made. … Well if we believe that basically all that science fiction they become our overlords anyway, like *Blade Runner* and stuff like that, so.

Jack accepts it, since:

> It is the age we are living in and we are moving to a more transparent time. So, I kind of get it, I am used to it; I think my parents would be, like, more, since they are not used

> to it they would be not okay with it, but [with] my age group, like, my generation, we have been sharing so much information, it is voluntary — we are voluntarily sharing this information. Even so, we know that this happens; we know that these companies take advantage of our information.

Some students are not in favor of data transparency, with Ryan declaring, "I don't like the concept, and I certainly struggle sometimes. When I stop and I think about it, how much of my personal information is out there, available to people?" and Abigail pondering:

> That is kind of like (...) like they know too much about me, in that sense, then they can literally, just by your, like, phone, a company can access so much. Apple knows where your home is, they know where you park your car … How do they know that information? If you have your phone connected to the car or whatever, and like, every time you are going somewhere, oh you are ten miles from home, but how do they know that is my home? … I don't like that because I am also a very private person.

Two students are ambivalent, as Owen says, "I am kind of in the middle [on] this because if the person allows it, if they want to have openly, on Twitter some people are just like, 'I am eating this, I am here today,' but it should be easier for people that want privacy." Ava pauses and sighs.

> I like it for me because I can tell what day and what time a picture was taken if I have location [services] on. I am not 100 percent happy with, you know, the fact that a company could sort of look through my photos because they are all up in the cloud or whatever.

The ethical, moral, and philosophical facets of data and personal information transparency were brought up by several American students.

Ryan reflects:

> I think, philosophically, the problem is that the information is mostly being held by corporations; it is not open to the public, which I would very much like to see. What is the information that is being gathered about me, what are the actual pieces of data that you have about me, who is gathering it, which can be really hard just figuring out in the first place.

Liam declares, "People should have the opportunity to keep their information private. I feel like it is not right, morally right [otherwise]." Harper complemented this thought by saying, "From, like, an ethical standpoint it is not, I mean for me, I don't know any ethics like theory, I think, but to me it is probably unethical to just keep so much information about people."

Luke feels that:

> The ethical issue has to be raised like it had to be more known like things how Edward Snowden leaked out the news on how the NSA is just tracking people, like spying on people, so I feel, like, what issue has to be raised? It has to be known to everyone if it is going to be even more transparent, like, basically, I mean, the people have to know it.

Owen also thinks that companies have a moral responsibility "so I cannot really say I would rely on the government to protect your privacy. So, unfortunately, I have to say the companies themselves, they have to look at it as a moral decision on their part." But he does not think that they actually have users' privacy in mind, as he states, "Because I don't think that it is in their best interest to make it easier for user to disable access to their data."

For some of the students, one way to address personal information and data dissemination is to have laws, regulation, or different policies implemented, with Luke suggesting:

> If people don't want to be in an ad[44] there should be an easy way, [so that if] our policy allows you to be in an ad, you can opt out. [Their] policy should be opt-in; it shouldn't be [that] everyone [opts in] automatically. It shouldn't be opt-out - it should be opt-in.

Harper adds:

> I don't think; however, it should be up to just the companies. I do think that it is also up to the government to protect [the] privacy of [its] citizens. So not just obviously America, I am talking about like all governments, that is their choice to do that, but obviously they don't have so much legislation over companies.

Echoing these statements, both Ava and Steve agree:

> So, we have a lot of laws about, like, [postal] mail, but we don't have the same laws [or they] don't necessarily apply to email, you know, so if someone took my mail out of the mailbox and opened it, I think that is against the law [she is laughing]. But if somebody, say, picked up my phone because I forgot to lock it and opened my email that is not illegal, so umm technically it is not that much different in terms of what you are looking at. So, that is why mean, that kind of legislation should catch up [with the times.] I do think there should be … I think there should be a little bit some more regulations and controls in terms of what kind of information companies can store and hold on to …

with Steve opining, "some stricter laws about security would be nice …"

Jack is the only student in favor of more protection for companies.

> I think, [don't] protect people but protect companies, so that data isn't stolen. They should have stricter laws to, like, keep the data within the company and not [allow it to

[44] He is referring to a rumor of Facebook being able to use its customer photos for ads: https://www.facebook.com/notes/facebook/debunking-rumors-about-advertising-and-photos/110636457130/

> go] anywhere else … I wouldn't like Snapchat sharing my information with other companies, but just Snapchat itself, because I am volunteering [it]. I know Snapchat is big and powerful and, like, they not using my data for "bad," so I would rather just share for them and no other companies.

For Luke, it is not only "something to do with the law can definitely be implemented, but I say more the education people should have like we should be more, we should know about it." Moreover, Harper proposes awareness as one way to better protect people's privacy:

> The change would have to come from a social standpoint; we just need to teach people not to give as much information out — they don't need to — and then it would force companies to realize [that] they cannot do that anymore because they are not getting the information they need. So, I feel like that is the only logical way which it goes from the people to higher up …

7.3.6 WhatsApp – German Students

Initially the plan for this thesis was to compare mobile privacy behavior and mobile privacy attitudes related to the messenger app WhatsApp. However, none of the US students were active WhatsApp users. Nevertheless, WhatsApp deserves its own subchapter, since the German students showcase distinctive mobile privacy behaviors and mobile privacy attitudes when it comes to this messenger app.

7.3.6.1 WhatsApp Mobile Privacy Behavior

Two WhatsApp users (Ralf, Ute) indicate they would prefer to either not use it all or at the very least use it less. Switching entirely to a more privacy-conscious alternative (in the students' opinion), such as Threema,[45] would be ideal for Ralf; he only uses WhatsApp to stay in contact with people not using Threema.

Beate and Berthold used to be WhatsApp users but switched to different messenger apps. As Berthold puts it, "I used it a bit on my previous smartphone, but then I uninstalled it ... and replaced it with Signal." *("Das habe ich auf dem vorherigen Handy eine Zeitlang benutzt, aber dann eben irgendwann deinstalliert … und mit Signal ersetzt.")*

Elke and Florian never used WhatsApp and have always relied on what they believe is a more private messenger app, Threema. Florian even purchased the app for his friends: "If one wants

[45] https://threema.ch/en

someone to use Threema, one has to purchase the first license for them." *("wenn man möchte, dass jemand Threema benutzt, dann muss man ihm die erste Lizenz kaufen.")*

Each of the six (Ralf, Wolfgang", Ute, Saskia, Jörg, Heike) regular WhatsApp users are aware of Facebook's and WhatsApp's data-sharing linkage (Muth, 2016). They all declined the option, as Wolfgang states:

> I cannot remember how it was, whether one had to tick or untick the box to disagree, but I did disagree … loads of my friends followed my behavior, they followed my decision, because they knew I had read the text and thus they didn't have to go through the hassle to read it too.
>
> *Ja, ich habe genau, ich weiß nicht mehr, wie rum es war, ob man den Hacken setzen musste oder ihn rausnehmen musste, um halt den zu widersprechen, aber ich habe dem widersprochen ... viele meiner Freunde haben es genauso gemacht, und sich dann nach meiner Entscheidung gerichtet, weil die wussten, ich haben den Text dann gelesen und dann mussten sie es nicht mehr selber machen.*

7.3.6.2 WhatsApp Mobile Privacy Attitude

Ralf is one of the students who would like to refrain using WhatsApp, as it is owned by Facebook.

> It is something — is it Facebook? — I believe Facebook owns WhatsApp and well, they have loads and loads of data [he is laughing], I don't like them, I don't use Facebook.
>
> *Das ist halt, war das Facebook, ich glaube, das gehört Facebook. und naja, dann haben die natürlich viele, viele Daten [er lacht], die sind mir jetzt nicht sympathisch, ich benütze jetzt auch kein Facebook aber.*

He prefers Threema; the fact that it is a paid-for, pro-privacy app[46] won him over. Also citing Facebook as the reason to use WhatsApp less often or at one point not at all, Ute assumes that:

> Because Facebook exploits my contacts and [perhaps] even more, it follows my connections more in order to better advertise to them.
>
> *Und weil Facebook ja auch die Kontakte mit auswertet und so oder noch stärker die Netzwerke nachvollzieht, und dann Werbung schalten zu können.*

[46] see https://threema.ch/press-files/1_press_info/Press-Info_Threema_EN.pdf

The reason why two students (Beate and Berthold) no longer use WhatsApp are because, in Beate's case, she doesn't like Facebook, and neither does she want to share her personal information and data from WhatsApp with Facebook. Berthold declares:

> Well, I think it is advantageous not to have all my personal information held by a big corporation, and thus I am trying … they belong to Facebook; that's why I am trying to not give all my personal information and data to those big corporations if I can avoid it. I try not to give too much of my personal data to Google, Facebook, or Amazon.
>
> *Aber denke ich, dass es noch von Vorteil ist, wenn man nicht zu viele Daten bei einem großen Unternehmen, und deswegen versuche ich schon […], die gehören ja zu Facebook, deswegen versuche ich, gerade von den großen Unternehmen meine Daten fernzuhalten, wenn es sich vermeiden lässt, also dass ich weder Google noch Facebook und Amazon zu viel von mir gebe.*

Beate shares this sentiment: she already uses Facebook Messenger and does not want one big company to receive her personal information and data via two different messenger apps owned by them.

> Well, I have Facebook twice, in a way, as a data aggregator, this doesn't have to be, and [Facebook] Messenger. Well, one has to use it now; it is no longer possible to use it via a [phone] browser. I used to use Messenger via browser, but that is no longer possible, and because of that I was thinking, "Well, I have to get rid of WhatsApp," because getting rid of it [means] I will lose only a few of my contacts, like real contacts, contacts I communicate on a regular basis with, and anyhow I don't have to give everything [to] Facebook. If I distribute it, I mean, I distribute it evenly onto different companies, that way one cannot start up a monopoly.
>
> *Ich habe aber zweimal Facebook quasi als Datenaggregat da, muss ja nicht sein und, wie gesagt, wenn dann denn schon und, wie gesagt, der Messenger war halt eben, den muss man inzwischen benutzen, man kann es nicht mehr über Browser machen, weil ich habe sonst immer viel den Browser benutzt des Messenger, das kann man jetzt nicht mehr und dann habe ich gedacht: Ja gut, da musst du dich halt von WhatsApp, weil da gehen mir am wenigsten Kontakte verloren, wirkliche Kontakte, wo ich sage, die höre ich halt regelmäßig, und trotzdem muss ich ja nicht Facebook alles hin werfen, also wenn, dann verteile ich das schon fair auf verschiedenen Leute, dann kann man zumindest auch kein Monopol mehr gründen – ja.*

Florian and Elke are the students that adamantly oppose using WhatsApp. Florian is suspicious of free apps and always wonders how free apps earn money. He doesn't want to become the product and, for him, the paid-for messenger app Threema is a pro-privacy alternative. He bought the app for all his friends:

> Well, if you think about it, I don't know too many people; I bought it for 10 people, it was maybe 17 euros, not really expensive.

Ich meine, wenn man sich das überlegt, da ich nicht so viele Leute kenne, das waren zehn Leute, das sind 17 Euro, das ist einfach kein Geld in dem Sinne.")

For Elke, WhatsApp belongs to Facebook and:

> About six months ago they released a press release acknowledging that data and information will be shared between Facebook and WhatsApp. Facebook initially promised not to do that after they purchased WhatsApp and, well, I think it is perilous to give all the communication data from my smartphone to a single company.
>
> *Es gab jetzt auch vor 'nem halben Jahr eine Presseerklärung, dass Facebook Daten und WhatsApp Daten doch in Zusammenhang miteinander gestellt werden, was bei der Übernahme ja noch irgendwie abgelehnt oder abgestritten wurde, also das halte ich für total gefährlich, dass dann ein Unternehmen alle Kommunikationsdaten, die auf meinen Handy passieren auf einmal.*

7.4 Mobile Security

As indicated in the research question this study's focus is not on mobile security. However as alluded in chapter 3, mobile security is distinct from but related to mobile privacy, thus it is not surprising the data analysis yielded some intriguing findings on this theme. Mobile security relates to malware, viruses, encryption, screen locks, and more on mobile devices.

7.4.1 German Students

Many German students have their phones' screen lock enabled, either via a pattern lock or PIN lock. Elke used to have a simple pattern lock, but after losing and recovering her phone at one point she set up a more complicated alphanumeric code. She believes that without the PIN:

> You can access my email; it is as if my email is not password-protected. One only has to enter the email into Amazon and [click] password reset.
>
> *Man kann auf meine E-Mails zugreifen, das ist wie, als wäre meine E-Mail-Account nicht passwortgeschützt. Man braucht ja bei Amazon nur die E-Mail-Adresse eingeben und Passwort zurücksetzen.*

During our interview, she also took pains to ensure that I never filmed her PIN, even though I assured her about the security and confidentiality of the recorded data.

Ralf chuckles when we talk about his PIN and says, "Well, you just recorded it, [I'm] pretty sure about that." *("ich glaube, den hast du jetzt auch aufgenommen, bin mir ziemlich sicher")*

He continues: "The phone is not secure at all, I mean [with the passcode] everyone can access everything." *("das ist ja überhaupt nicht sicher und da kann ja jeder ran, wenn er will.")*

Florian remarks that he set up disk encryption on his phone, but discloses that his SD card is not encrypted. According to him, none of the photos he stores on the external SD card are of relevance or importance to anyone but himself, and therefore he does not feel the need to encrypt his SD card. When I ask him if he has antivirus software on his phone installed, he says no.

Berthold speaks in great detail about his various security setups. Most of his apps need a password: "All the things I don't want anyone to have access to but me, these are secure." *("Ja, also die Sachen, bei denen ich nicht will, dass niemand außer mir selbst Zugriff hat, die sind auch entsprechend gesichert.")* For example, the messaging app Signal logs him out after three hours of being idle. He does not use an email app because he thinks they offer inadequate security measures; he only accesses his email via his mobile web browser. Overall, Berthold seems to be very security-conscious regarding his phone. Yet he confesses to not having his phone encrypted.

Jörg openly professes that he used to have a four-digit screen lock set up, but he found it too tedious to enter and eventually removed it: "I reduced my data protection because I am lazy." *("Da habe ich selber den Datenschutz verringert aus Faulheit.")* However, in his opinion, mobile phones are less secure than computers. He does not use mobile banking on his phone and generally thinks that public awareness on how to secure your phone from hackers needs to improve. He recommends installing an antivirus program on a smartphone.

Backing up their phones to their computer is another security decision two of the subjects (Jörg and Beate) bring up. Both prefer not to use cloud storage services, but rather back up their data directly to their computers.

Beate, Florian, Jörg, Heike, and Elke confuse privacy and security and demonstrate some security options during the experiment part A.

7.4.2 American Students

Ryan and Owen both mention malware, which is why Owen keeps his mobile operating system current. He also talks about Stagefright,[47] which is a software bug in the Android system. However, these two students also confess to not having a screen lock set up for their phones. Ryan says that he does not see the point of it, since his phone is on his desk at work or home, or it is in his backpack. Owen used to have a screen lock set up, but found it very inconvenient and:

> It was such a basic password I wondered if this even protection, because my password was this [shows me a swipe on his screen]; it was such a simple password anyone could possibly — I am not saying anyone can just guess it, but it was not exactly the most complex [password].

Overall though, the majority of students have a screen lock set up, either as a fingerprint or PIN.

Harper points out that several of her apps, mostly the ones she uses for financial transactions, require her to enter a username and password. Marsha will not enter a credit card on her iPhone and does not have Apple Wallet set up either:

> I guess I just don't trust sharing credit card information over my phone. Like, I also really try to avoid entering credit card information if I am on a public Wi-Fi [connection], there never has been anything urgent that I cannot wait until I get home.

Backing up the content of their phone is another security precaution utilized by Jack and Ava. Ava and Jack both backup their phones via the cloud as well as on their computers. Moreover, both also backup their computer to an external hard drive.

Ava's Android phone once got stolen from her dorm room. She thinks iPhones are more difficult to steal because they are trackable via the Find my iPhone app.

Ryan, one of the students without a lock screen, does have "Google's locate and disable features, so I could, if it disappeared, I could look it up and lock it down if I needed to."

Two American students (Ryan, Abigail) confuse privacy and security during the mobile privacy setting part of the app experiment with Abigail wondering, "I don't know why, I just think it gives me ideas. I think it is more like, just like protecting your phone from, 'cause, like, phones are hackable, too."

[47] https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

7.5 Linguistic Highlights

The following subchapter organizes into themes some of the linguistic highlights that have been part of the thick description. Particular emphasis will be given to words, phrases, and nonverbal cues that highlight participants' feelings and emotions about mobile privacy.

7.5.1 German Students

On privacy:

Beate:

> **It kind of sucks;** if the internet knows, one cannot deny that it ever happened or say, "Well, that was a long time ago."
>
> **Dann ist es natürlich Scheiße,** wenn das Internet das weiß, weil dann kann man es nicht abstreiten, man kann auch nicht sagen, das war einmal.

Heike:

> **It feels a bit creepy, a bit "Big Brother is watching you"**. I always used to say, "I don't care because I have nothing to hide," but then I found out that is a common saying uttered by many people, but of course that doesn't mean you want the entire world to read your emails. (Heike)
>
> **Fühlt sich einfach so ein bisschen gruselig an so "Big Brother is watching you" Ding ... früher** habe ich immer gesagt, ach ist mir doch egal, ich habe eh nichts zu verbergen, wie ich mittlerweile rausgefunden habe, so ein Standardsatz von den meisten Leuten, aber natürlich möchte man trotzdem nicht, dass die ganze Welt deine E-Mails lesen kann.

On location-service attitude:
Wolfgang:

> Theoretically, if it is not turned off, it is possible to see where I am and where I am going. I really **find that creepy;** it is like someone is always watching me.
>
> Also, zum einen kann rein theoretisch, wenn man es halt nicht ausstellt, immer geschaut werden, wo ich bin und wo ich mich hinbewege, und das finde ich halt **tatsächlich wirklich creepy [sic],** das ist so als ob mich jemand verfolgen würde die ganze Zeit irgendwie.

On the app experiment: Perfect Piano behavior and attitude:

Ralf:

[I] want to know, if I install the app, what does it get from me? **[he is laughing somewhat artificially]** Nothing in life is free **[he is laughing]** … and I think, "Why does it need to access my files or my calendar?" or whatever, and then I think, "Whatever; well then I won't install it."

Weil ich mir manchmal, ich möchte halt wissen **[lacht etwas künstlich],** was die von mir kriegt wenn ich die installiere ,weil nix im Leben ist umsonst" **[er lacht]** … mir denke, warum brauchst du denn den Zugriff auf meine Daten oder auf den Kalender oder auch sonst, was denke ich mir so nö, also dann installiere ich die halt nicht.

Beate:

So that's why I **sorta get suspicious.** Usually, if the app asks if it can access my media and files, well, usually I try to say NO, and sometimes the app functions without it, and sometimes it doesn't function without it, and then I weigh, "How urgently do I need the app?" But usually my rule is to deny access to my media … well, for me that is the most personal thing on my phone. … I think so, I mean, it is more personal to me than my messages [she clicks on deny].

Das ist halt das, was ich meine, also da werde ich immer ein **bisschen spitzfindig**, also in der Regel, wenn mich jemand fragt ob er auf meine Medien und meine Dateien zugreifen will, versuche ich immer erstmal zu sagen, NEIN, so, und die Frage ist manchmal funktioniert es auch ohne so und manchmal geht es auch nicht ohne, und dann schätze ich ab ok, wie wichtig ist es mir gerade, dass ich das wirklich haben will, aber in der Regel lehne ich gerade Zugriff auf meinen Medien halt ab, weil es halt das Persönlichste an meinen Handy ist, würde ich mal sagen, also ich glaube sogar manchmal persönlicher wie die Nachrichten, die ich da drauf habe. [Sie klickt auf Verweigern]

On app experiment: favorite app behavior and attitude:

Heike:

This app [Facebook] has access to the following functions. **Wow, that's quite something [she chuckles]:** status and identity, read your text messages, that is new, if you have Facebook Messenger, then it shows your regular text messages, too. I don't want it, but I cannot change it. Photos and media files [she scrolls farther], exact location, contacts, email [she scrolls farther], **they really have everything [she is laughing hysterically].**

Diese App [Facebook] kann auf die folgende Funktion ihres Telefon zugreifen, oh ist ja **krass oder [sie lacht leise],** Telefonstatus und Identität, Textnachrichten lesen, das ist jetzt ganz neu, dass man, wenn man hier diesen Facebook Messenger hat, dann werden da auch die SMS angezeigt, will ich eigentlich gar nicht, geht aber nicht mehr anders, Bilder und Videos Audio, [sie scrollt weiter durch Einstellungen von Facebook

app], präziser Standort, Kontakte, email, [sie scrollt weiter und liest], **die haben echt alles ne [sie lacht hysterisch].**

On privacy policy attitude:

Wolfgang:

> … If someone wants **to harm me** and they want to protect themselves legally, well then, they could write harmful/nasty things into the wrong paragraphs, hoping that I don't read it.
>
> ...Wenn jemand mir **wirklich was Böses will** und sich rechtlich absichern möchte, dann schreibt er halt im Kapitel, wo es eigentlich nicht richtig reinpasst halt, die schlimmen Sachen rein, in der Hoffnung, dass ich es dann nicht lese.

On personal information and data–attitude:

Wolfgang:

> Well, theoretically of course, my cell phone provider, I mean it has to be like that so that everything works. **But it is a bit creepy** if I set up my cell phone, I receive a text message from my mobile phone provider, and my phone is being set up without me being involved at all.
>
> Also theoretisch mein Mobilfunkanbieter natürlich, der sowieso, das ist so, ich meine, muss ja auch, damit das alles funktioniert, **aber es ist halt so ein bisschen unheimlich halt,** wenn ich das Handy halt neu einrichte, dass ich dann von meinem Anbieter eine SMS geschickt bekomme, die dann von meinem Telefon automatisch, ohne dass ich was tue, interpretiert wird.

On the transparent human- attitude:

Heike:

> Well, first and foremost, I find the term "transparent human" **a bit scary because** … right now, the development — and I am not talking about smartphones only; for example, your shoes have a tracking device, as does your car and everything else — means someone could follow my entire life, when ultimately it is nobody's business.
>
> Ja, also in erste Linie finde ich erstmal der Begriff "der gläserne Mensch**" erfühlt mich erstmal mit Unbehagen,** weil ... weil im Moment entwickelt sich das alles in so eine Richtung, wo man also, das geht ja nicht nur über das Handy, dann hast du an deinen neuen Schuhen noch so ein tracker Dingsbums dran und im Auto und überall, könnte man dann dein ganzes Leben nachzeichnen, und ich finde schlussendlich geht das eigentlich keinen was an.

7.5.2 American Students

On mobile privacy:

> Hmm (…) I don't think I have any privacy in terms of the apps that I use; they collect a lot of information – they've got access to everything, they know more than my girlfriend, my parents too, to be honest. Yeah, but how do I feel about it? I think since we are talking about it, it is a **little sketchy, it is a little weird, but,** in the moment, when I am using the app, I don't really mind. (Jack)
>
> I know that the people who developed the phone. or Apple, they can have access to whatever they want, really. **Kind of scary,** but it is interesting, I guess. (Liam)

On the location service attitude:

> They want to be able to collect everything from everyone all the time. Why would you need that? **It is scary that it is out there**, that they're building the capacity to be able to monitor everyone all the time. I don't know … (Ryan)

On the app experiment: Perfect Piano behavior and attitude:

> Right [he went to the Google Play Store and looks for the app now] then I search for it, then I usually browse through the reviews. If I don't know the app and I see it has a 4.2 [stars] so I download it […] Yeah, I think my limit would be if I saw 3 stars**, I would be suspicious**, I'd probably think the app is useless, maybe I'll read through reviews and see if it says "This app is bad it because it pops ads onto your screen." (Owen)

On the privacy-policy attitude:

> "Typically think they **try to deceive people** with the length. I know they probably do sometimes; they probably get away with a lot of things." (Marsha)

On the personal information and data – attitude:

> ... You never **really know if they are actually doing something dark or anything, they could be … like, invading your privacy**. They are using it for the betterment for themselves and not so much the … basically they don't consider, like, the other people, so they use it for their own benefit just to gain profits or something like that. But they usually use it for like predictive analytics; yes, they try to predict consumer behavior, like they try to find the best way in order to serve them better, so it is all about analyzing data. Like, Facebook, they probably do like some kind of emotional trend [analysis], because they are basically an information provider, so they are not necessarily just a social networking website. So, like, they just try to track to see how people, yeah like how information, like how the news actually affects people. Sometimes they can even alter someone's News Feed to [make them feel] more happy [sic], that can actually affect if the person becomes happier, so they can manipulate certain data and like that. (Luke)

On the "transparent human" (*Der gläserne Mensch*) – attitude:

> I mean, when you think about it that way, **I guess it is scary in a way because anyone that can get through to their servers or their systems can have access to you.** But at the same time, for example, Twitter and Instagram, they are for entertainment [purposes], and they [improve] your quality of life better, so, for the most part, I access it. You kind of disregard that, put it on the back burner, kind of concentrate on what entertainment they provide to you and, yeah. (Liam)
>
> Umm, am I actually okay with it? **No. Do I feel like I need it, [that] I need to not worry about it in order to survive in this kind of environment that we live in? That is a different question [she is laughing] … and I don't like [it]** but I don't think I have a choice anymore as to whether not I can like it or not, **which is terrifying** but at the same time … (Harper).
>
> It is a **technical monopoly but it is not a *monopoly* monopoly, like J. D. Rockefeller** and that type of thing … We are living in an age where privacy is a rare thing **... so far Big Brother hasn't rolled in the squads yet.** Well, it is a good think to keep in the back of your mind to not let the government go too far**, there is a reason why that book [*1984*] was made. … Well if we believe that basically all that science fiction they become our overlords anyway, like *Blade Runner* and stuff like that, so. (**Steve)

7.6 Chapter Summary

In this section, the findings have been told via two composite narratives as well as different topics. The chapter that follows moves on to describes Fieldwork 2 discoveries.

8. Findings Fieldwork 2

8.1 Overview

In this chapter, the findings originating from the data analysis are organized by the following themes:

1. Facebook scandal
2. General Data Protection Regulation/GDPR
3. Privacy protection
4. Privacy education

Additionally, two subchapters highlight mobile security and linguistic occurrences. Even though the linguistic expressions, phrases, and sentences are already included as part of the thematic descriptions, they warrant highlighting.

In the following chapter 9 the terms "privacy education" and "privacy protection" are used instead of "mobile privacy protection" and "mobile privacy education." Although the focus remains on mobile privacy, many of the concepts and implications also apply to privacy in all of the digital world.

The respondents were renamed to avoid referring to them by their code. Since the four interviewees, two in Germany and two in the US, already participated in Fieldwork 1, the same names were used (see Table 18):

GSF1	GSF2	ASF1	ASF2
Beate	Jörg	Steve	Ava

Table 18 Alias names of the four interviewees

8.2 Findings by Themes

8.2.1 Facebook Scandal

The Facebook Cambridge Analytica scandal[48] received a lot of worldwide media attention. As indicated in the Research Method chapter, when the news broke, Fieldwork 1 was still in its analysis stage, providing the opportunity to initiate a follow-up study to research and investigate questions like the following:

- Do German and American participants have different perspectives on the scandal?
- Did the scandal impact their behavior and attitudes toward mobile privacy?
- Do they think about mobile privacy on their smartphone (or on Facebook in general) differently due to the scandal?

8.2.1.1 German Students

Chuckling, Beate says that she was not surprised by the Facebook scandal. To her, it was always very clear how Facebook makes a profit: by selling her personal information to other companies. She cannot recall the exact details about the scandal, and speculates whether Facebook had been hacked or if Facebook sold users' data without their consent. Relating the Facebook scandal to our first interview, she openly admits that she still has some apps installed on her phone that track and harvest her personal data and information — which she acknowledges makes her personal information vulnerable to being hacked, sold, or abused in the future.

Facebook's response to the scandal left her somewhat bewildered, as Facebook now "pretends" to be overly concerned about its users' privacy. She tells me that all over Berlin, Facebook billboards advertise how to protect one's privacy. According to her, this is insincere because:

> [Facebook] know they just screwed up and now they are trying to [earn] that trust back. Furthermore, I think that's just really ridiculous. I stand in front of a billboard and think, Well, my ass [laughing]; well, I made a pact with the devil when I created a Facebook profile."
>
> *Sie [Facebook] wissen, dass sie gerade Mist gebaut haben und versuchen es, so ein bisschen wieder reinzukriegen, dieses Vertrauen. Und ich finde das halt eigentlich super lächerlich, eigentlich halt. Na, also ich steh dann da immer davor und denke mir,*

[48] https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

verarschen kann ich mich auch selber [sie lacht laut], also ich habe ein Pakt mit dem Teufel geschlossen, als ich ein Facebook Profil angelegt habe.

Nonetheless, she still uses Facebook because:

> [When] someone has a monopoly, it doesn't matter if it is physical or digital: they have the spending power, and that's how it is with Google and Facebook — there are no real alternatives, no alternatives, at least, that are as good and or as fast.
>
> *Leute, die ein Monopol haben in irgendeiner Form, egal ob digital oder real, die geben halt die Kaufkraft an, und bei Google und Facebook ist es halt genauso, es gibt halt nicht so die wirklichen Alternativen, die genauso bequem und genauso schnell sind.*

Beate never took the steps necessary to verify her privacy and security settings on Facebook. She maintains she has always been careful with her privacy and security settings and with what she shares online. She tells me that she no longer uploads any pictures of friends who are not on Facebook or photos of children, in an effort to respect their privacy. However, she acknowledges that:

> Sometimes I have a bad conscience because on my smartphone, well, I have all these photos of my family, and sometimes I think, "Well, maybe I should take these off at regular intervals, just to make sure they are no longer on my smartphone." And, well, as I said earlier, with all the other stuff on my smartphone, it doesn't matter to me, but if [my information was exposed] I would [feel as if] Facebook manipulated me somehow, and usually one only notices it after the fact.
>
> *Da habe ich schon manchmal ein schlechtes Gewissen, wenn ich es auf meinem Handy, da habe ich Fotos eben von meiner Familie, und so, wo ich mir schon manchmal denke, vielleicht sollte ich die regelmäßig runternehmen vom Handy, und dann auch gucken, dass ich die regelmäßig nicht auf dem Handy habe, wie gesagt bei allen anderen ist es mir egal, was ich auf meinem Handy mache, aber wenn etwas passieren würde, wo ich auch merken würde, da hat Facebook mein, mein, mich manipuliert auf eine Art, was man ja auch irgendwie immer erst weiß, wenn es klar wird, dass man manipuliert worden ist.*

Generally speaking, Beate considers herself to be a conscientious app installer, often weighing the pros and cons of having her personal information shared and/or tracked by a company. In Beate's opinion, this is the trade one makes for a free app or services. But she confesses that most of the time, convenience wins any argument.

> I have to admit, I ignore it or I think it is not bad because it is so convenient. I mean, it is like that with many apps. It is like horse-trading or like [making] a pact with the devil. What are the benefits and what are the risks; how could it become harmful to me in any way?"
>
> *Auf manchen Schienen ignoriere ich es oder denke ich immer, das ist nicht so schlimm, weil es bequem ist, und das ist halt bei vielen Apps nach wie vor so. Dieser Kuhhandel*

oder dieser Handel mit dem Teufel quasi. Das ist dann immer so, was bringt es mir und wie groß ist die Prozentwahrscheinlichkeit, dass es mir irgendwie schadet.

Referring back to the monopolies of Facebook and Google, whenever possible she avoids giving Google and Facebook access to the personal communications on her phone:

> Google and Facebook, you can have my data, but it is enough if they have access to it via one source. It doesn't have to be [through] my private conversations — one source is enough.
>
> *Google und Facebook ihr könnt meine Daten gerne haben, es reicht auf einer Quelle, aber es muss nicht meine private Konversation sein, es reicht eine.*

Beate also points out that she would be willing to pay a small user fee for Facebook if, in return, Facebook would guarantee privacy protection and not share anything with advertisers and/or third-party applications.

> I would love it if Facebook would offer a paid version. Once a year, one could pay one or two euros, but then we [Facebook] won't need your personal information. I wonder why Facebook is so afraid to charge a price; with WhatsApp, it used to be [that] they [charged] 90 cents [for] a paid version, and in return [said], 'Oh well, no access to your personal information then.'
>
> *Aber ich fände es einfach schön, wenn Facebook die Möglichkeit geben würde zu sagen, du bezahlst jetzt einmal im Jahr einen oder zwei Euro, und dafür brauchen wir [Facebook] erst gar nicht diese Daten. Weil das ist halt auch immer meine Frage noch, warum sich Facebook so sehr ängstigt davor, mal ein bisschen Geld, bei WhatsApp war es ja schon so, dass es sie sich getraut haben, 90 Cent zu verlangen, irgendwann mitten drin, aber ich glaube den Leuten anzubieten oder zu upgraden auf eine Version die halt was kostet, aber dafür eben zu sagen, gut bis hierher und nicht weiter.*

Trust is another issue: "Even if I told Facebook that I don't want them to share my data with any third-party source […] honestly how will I ever find out if they do it or not?" *("Nur, weil ich bei Facebook vielleicht gesagt habe, ich möchte meine Daten nicht mit irgendwelchen Drittanbietern teilen. Ob die das tun oder nicht, ne also … Wie werde ich es erfahren?")*

Jörg ponders for a bit before he says that even before the scandal he was quite knowledgeable about security. The scandal confirmed his preconceived notions about how vulnerable his personal information and data is and how it can be abused. To him, this could be because of hacking, company neglect, or because he was careless. Jörg thinks that having one's information and data open to unwanted intruders is part of a trade-off — in return, he receives free services.

Regarding the details surrounding the scandal Jörg is not quite sure what exactly happened. Jörg vaguely remembers that either an advertising company or Facebook partner abused user data without previous consent from Facebook. In his opinion, the reputation of Facebook — or, more precisely, the reputation of its CEO, Mark Zuckerberg — has not been tarnished. In fact, quite the contrary; to him, during the Senate hearings, Mark Zuckerberg was:

> In charge, [as] the members of the Senate seemed to be misinformed, and sometimes they didn't even know what Facebook is and how it works. And that's why [Zuckerberg] had a lot of loopholes and they couldn't really grill him too much.
>
> *Die Senatsmitglieder sehr schlecht informiert waren, teilweise gar nicht wussten was Facebook ist, wie es funktioniert. Und dadurch hatte er [Mark Zuckerberg] natürlich gute Schlupflöcher beim Antworten und dadurch konnten sie auch nicht wirklich tief bohren.*

Jörg also thinks that Facebook took the necessary steps to make amends and does care about the security of their users' information now.

> Hmm … oh well, I was quite aware before it, in terms of security, but it confirmed my perception that all data and personal information, which are part of a deal in exchange for a free service — well, they really can be hacked. It doesn't matter how; if it's a professional cyberattack, or if it's because of carelessness, or one's own fault.
>
> *Hmm … Also ich hatte mir ja schon vorher ein relativ starkes Bild glaube ich auch gemacht, was Sicherheit an betrifft und das hat mich in meinem Bild glaube ich auch nochmal bestätigt für mich selber, so das ich dann gesehen habe, gerade die Daten die ja hinterlegt sind, mit denen man ja im Prinzip handelt und sich kostenlose Service erkauft, das die wirklich teilweise angreifbar sind. Egal von welcher Seite, ob das nun ein Hack ist der professionell erfolgt oder durch Unachtsamkeit oder eigenes. Ja das beschärft mich nochmals in meinem Bestreben.*

Although Jörg is a WhatsApp user, he does not have Facebook installed on his smartphone. This is not due to the Facebook scandal, but because WhatsApp is owned by Facebook, and he does not want both free services to be able to share his personal information and data. Jörg does use Facebook sporadically on his PC, and admits to not verifying his security and privacy settings after the data breach scandal.

> I relied on the fact that I already had it set pretty securely … I did not check it again, and I did not check to see if there are new [privacy] options.
>
> *Ich habe mich irgendwie darauf verlassen, dass ich das vorher schon relativ restriktiv eingestellt habe. Aber nein, ich habe es nicht nochmal überprüft und ich habe auch nicht nochmal überprüft, welche neue Funktion es gibt.*

Jörg views himself as a thoughtful, careful smartphone user and tries to limit the number of new apps he installs on his phone. However, he just recently downloaded a blood donation

app developed by the German Red Cross. He did not mind entering his personal information and data into it, since it is for a good cause. Overall, he would like to become more privacy-conscious on his phone; for example, by replacing WhatsApp with Threema and using DuckDuckGo instead of Google. He has not yet installed or tried out these alternatives, most likely because he hasn't had the time.

Concluding our conversation about the Facebook scandal, Jörg touches on a privacy incident that occurred during a new-employee onboarding week. Jörg received work-related text messages on his private WhatsApp account, and was a bit puzzled and annoyed. He then felt forced to update his casual profile photo and status biography to a more professional one:

> I was pretty pissed … I experienced firsthand how my workplace doesn't respect data privacy too much. I didn't like [the fact] that … my account was linked to my personal phone number.
>
> *Und da war ich schon ziemlich stinkig, Da habe ich selber gemerkt das selbst auf Arbeit bei uns, das mit dem Datenschutz nicht so gehandhabt wird, das fand ich nicht okay, weil ich da mit meiner Privatnummer vertreten bin.*

Jörg's overall philosophy is that smartphone users have to be attentive, vigilant, and cautious about the apps they install on their devices. Even if a company promises to protect data and information, he believes that *all* systems are hackable and therefore vulnerable.

8.2.1.2 American Students

Steve has heard about the Facebook scandal and says that, for him, it was tacit evidence that Facebook was recording users and obtaining personal information through their on- and offline interactions. It was an open secret that Facebook was "using some software to record its users, and, of course, nobody exactly likes the idea that they are being recorded. Even though you kind of *do* know it in the back of your mind that they are doing it. But, of course, now that it is official everybody is getting upset." The scandal made him more fearful about what he posts through his phone. He admits that it does not feel good to know that, as a user, all of his data and information is trackable and hackable. "It felt … it certainly didn't feel any good. It basically just made me fearful of what I kind of post on my phone." In his eyes, Facebook's attempt at damage control did not make him feel better: "Like ‘all these journalists will work with us,' that kind of thing … it is [the] overinflated self-importance that makes

people not like Facebook more." However, he sighs and pauses for a bit and then says that everyone, including him, is still using Facebook because of the convenience. At this point, he adds, if he were to do anything "bad," Facebook would already know about it, so *not* using it does not change anything.

After the scandal, Steve did not check any of his privacy and security settings on Facebook, nor did he find the time to go through the settings to see what apps he has connected to his Facebook account. "I am pretty sure many people are sort of like me, where we understand that we *should* do this, but we have a lot of other stuff going on." He knows that he should check his Facebook settings, but is always too busy to do so. He also believes that nothing is going to change: "Like, as I said, what Facebook was doing was basically an open secret; they are the ones that got caught just now. But unless some sort of huge scandal happens again, that exposure … it is official that Google and Co. are doing this, [and] they are not going to stop."

The second American student, Ava, does not remember what the Facebook scandal was about. She remembers Mark Zuckerberg being called in front of Congress but does not recall the specifics. She wonders, "Hmm, I cannot remember if it had something to do with information that was not being kept securely. I don't remember if it had to do with the Russian hackers? [laughing] I honestly don't really remember the details."

Ava also mentions, "I mean, I knew after our conversation that [apps] were kind of tracking me or that they kind of trick you in [order] to get more information on you." She still uses Facebook, as she does not "really worry too much about my information still. [It] doesn't really bother me that much. I mean, I get tracked and I know that, and I do not want [people to get a hold of] certain information … but it does not really bother me so much that [the] information gathered on me is used to market [stuff to me] in general."

Nevertheless, she checked her privacy and security settings on Facebook even though she felt it was pretty secure and private before the scandal. Contradicting her earlier statement that she did not care if information is shared, "I just feel it is not a good idea to have so much personal information on the internet." She still uses her Facebook account to log into a lot of apps and websites, as "almost everything is connected to my Facebook account, and I purposely connect things to Facebook because I do want the convenience of being able to log in quickly and not have to type my email and [remember] multiple passwords. Sometimes I

am a little worried about that, because if someone did hack my Facebook account, that would be really bad. So, I have a pretty complicated password for Facebook. I haven't changed the email, [even though] it is not the best email. It is a Yahoo email [account] and Yahoo has had problems with security." Sometimes it makes her a bit nervous as she "logged in with something and deleted the app and who knows who's got the data [laughing]. That is kind of scary [laughing]." Wrapping up her thoughts on Facebook, Ava tells me that she was a grader for a communication class and how, as an assignment, students were asked to Google themselves and write an essay about their experience. After reading these freshmen essays, her general observation was that the younger generation seems to be:

> A bit more "aware," and a lot of them proclaim to be more private in the essays that they write for me [laughing] … Yes, they say they really worry about posting stuff and I have noticed there [are] some people that post almost nothing on social media. So maybe some of them really are more aware and more worried about what they put out there and maybe more worried about some apps.

8.2.2 General Data Protection Regulation (GDPR)

The European General Data Protection Regulation (GDPR) became official law on May 25, 2018. In the months leading up to its implementation, it garnered worldwide attention from both the media and scholars.

> The GDPR now sets a standard which is to be taken as a clear statement by the biggest single market in the world. No data controller will be able to ignore this and other governments will be under pressure to raise their data protection standards in order to allow their economies access to the digital single market of the European Union. (Albrecht 2016, 288)

8.2.2.1 German Students

Both German students remembered that they had received many updated privacy policies, either via email or on websites, following the implementation of the GDPR.

Beate exclaims, laughingly, "phew, I really got a lot. I didn't know I had so many different accounts." *("BOA. Ob ich welche erhalten habe. Mir war gar nicht klar wie viele Konten ich habe.")* Beate claims that she tried to read all of the privacy policies. She also tried to turn off many default settings, at least for all of the accounts she uses in her everyday life.

Yahoo's privacy policy update and settings annoyed her, because it seemed like a purposefully complicated and off-putting process: "It was pretty tedious; one noticed how much they [Yahoo] did not want one to understand it." *("Das war richtig gemein, da hat man auch gemerkt, wie sehr die [Yahoo] das nicht wollen, das man da rauskommt.")*

She also comments that she even received updated privacy policies for services or accounts that no longer exist. For example, she found it very surprising to receive an email from Netlog[49] informing her retrospectively about her account being part of a data breach:

> … And I had an account, and I received an email from Netlog around the time the privacy law came into place, that they had folded in 2012 and the company had merged with another company but some data breach had occurred back then and my account was part of it. And I had to remind myself about Netlog.
>
> *… Und da hatte ich ein Konto und jetzt, also kam eine E-Mail von Netlog, so in der Zeit von dem neuen Gesetz, dass sie 2012 also zugemacht haben und zu einer Mutterfirma gezogen, dass da wohl Daten geleaked [sic] worden waren und dass mein Konto dabei wäre. Und dann saß ich da und dachte mir Netlog?*

The other German student, Jörg, says he skimmed through some of the updated privacy policies but did not read all the details. He brings up an incident exemplifying how both companies and individuals were confused before the regulation went into effect. His physiotherapist would no longer allow him to make an appointment on the phone unless he signed the updated privacy policy in person. According to him, in the month leading up to new regulation, many companies and many people were annoyed and confused. They did not perceive it as something beneficial. It was more of a hassle that created more work: "And they were all upset because it created a lot of work, they did not see the benefit of it." *("weil sie haben sich eigentlich nur aufgeregt, weil für sie ist das eine große Beschwerde ist. Aber haben gar nicht den Nutzen für sich da gesehen.")*

Neither student knew specific details about the new data privacy law, but both welcomed the debate that GDPR spurred in public and in private.

Jörg assumes Germany was already well ahead of other European countries in regard to data privacy laws. "So, in principle, other countries have followed suit, so to speak. With us here in

[49] https://oag.ca.gov/system/files/Communication%20to%20Users%20-%20FINAL_0.pdf

Germany not a lot has changed." *("Also, im Prinzip haben andere Länder nachgezogen, sind sozusagen, bei uns in Deutschland war jetzt nicht viel, was sich geändert hat.")*

He also favors keeping the law current and updating it in-line with technological advancements:

> One just has to be careful that the legal protections for citizens in terms of privacy stays ahead, because AI [artificial intelligence] and digitalization will continue to evolve and therefore laws have to be quickly implemented. What you need are larger task forces, a lot more awareness, and a lot of lobbying work.
>
> *Man muss einfach da aufpassen, dass der gesetzliche Schutz der Bürger der Privatsphäre, der muss einfach immer mitziehen, weil die KI [Künstliche Intelligenz], die Digitalisierung wird sich weiterentwickeln, ebenso schnell müssen die Gesetze ran, da braucht man eben größere Arbeitsgruppen, viel Bewusstsein, viel mehr im den Fall durch Lobby Arbeit.*

Beate mentions her roommate's boyfriend, a lawyer who happens to specialize in data protection. According to him, the new law was overhyped by the media and that "to be honest, the law is a nice idea, but it is incomplete and moronic, and it is … well, it doesn't really help either, that's what he said." *("Also, wenn man mal ehrlich ist, das Gesetz ist ja eine nette Idee, aber das ist so lückenhaft und, dass eigentlich … aber so richtig helfen tut es auch nicht. Es ändert nicht wirklich was meinte er dann.")* As a user, she still finds it too difficult to understand where her data is and what a company is allowed to do with it, as it:

> Is an obtuse structure, is non-transparent, the whole thing. Even if I would say I know what data Facebook has, I can never figure out what they are legally allowed to do with it.
>
> *Eine undurchsichtige Struktur, ist so Intransparenz das Ganze, das selbst, wenn ich jetzt sagen würde, ja, ich weiß, welche Daten Facebook hat, ich könnte nie einschätzen, wo die landen vom Gesetz her oder was die damit machen dürfen.*

Jörg comments[50] on how so many things have happened, such as the GDPR and the Facebook scandal. But he confesses that these things do not seem to have had an impact on people's behavior:

> … well yes, it is true, if Google wants something, I just scroll down and click continue. A lot has happened concerning your topic, but it doesn't impact people's behavior [laughs quietly], but well yes, a lot has happened.

[50] During the interview debriefing part

Ja das stimmt, immer, wenn Google was von mir will, scrolle ich auch immer runter und sage weiter. Es hat sich viel getan für dein Thema, nur dass es keine Auswirkungen [er lacht leise] hat offenbar auf die Leute, aber ansonsten ist ja relativ viel passiert.

8.2.2.2 American Students

Both American students remembered receiving numerous updated privacy policies in the months before May 2018.

However, Steve confesses, "Yeah, I have noticed that there were updated privacy policies, but just like how nobody really has time to go all these complicated settings, nobody is going to read the privacy settings and stuff. The only thing I really follow is that you need to be a lot more careful about what you do online."

Ava notes that she read some updated privacy policies, either because she received them via email or because she was forced to read them before proceeding to the website:

> I have. I think there was kind of, there was something that passed about security protections legally, not that long ago. There is this one website that I really like, it is called Archive of Our Own,[51] actually it is connected to an academic journal and it is this whole organization for transformative works, I think it is called. And they sent — it wasn't in their email, they have a feed on their main page — that [read] there have been some changes in the EU, something about security changes and most of the people visiting the website are from the United States, but here is what we want you to know [regarding] what we do for security and they gave some information about that. It is probably still there.

Ava also mentions some sites where she was, by default, logged out and had to read the updated privacy policy before logging in again. She remembers one particular website[52] where:

> They had a really interesting style of writing: like, their formal stuff … usually websites kind of make it dry, or they kind of try to make it witty and funny. That is their style so they were like, "We just want to make sure that you actually saw this and that you actually take the time to read it because we know that most people just scroll by it." So, I kind of appreciated that and I scanned it and because many of their members are focused on being private.

Steve thinks that the flood of updated privacy policies was related to the Facebook scandal:

[51] https://archiveofourown.org/

[52] https://fetlife.com

> Basically, they want to avoid a big scandal [like the one] that Facebook is going through. Like, I understand that is primarily the reason. They don't want to be caught in this whole thing. If people, like, call them out on it, they can be like, "Hey, look, you signed the privacy settings saying yeah, we can do this. Thus, it is not our fault."… Yeah, basically they just doing, like, damage control and trying to mitigate any future scandals.

When I inform him[53] that a new European data privacy law is the reason for all the updated privacy policies, he perceives it as a step in the right direction. For now, it is still going to be:

> …Nothing. Of course, you know the FCC is, as of this moment with the current administration, primarily motivated by profit and all that. However, the more people harangue them and place similar laws and the more younger [sic] people get in, you cannot, you know, use laws from years ago with the current tech advancement and hackers and all that. There will be improvements and they might take some notes from the EU's current standards.

Ava is aware of a new European law that passed related to privacy protection. However, she does not think that under the current Trump administration similar legislation will be put into effect in the United States.

8.2.3 Privacy Protection

The public and scholarly debates in the months before and after the GDPR implementation, combined with the Facebook scandal, emphasizes how privacy protection cannot be ignored and is a primary concern for businesses and governments alike. Furthermore, according to Boerman, Kruikemeier, and Zuiderveen Borgesius (2018):

> People are concerned about their online privacy, worry about possible misuse of their personal information, and express the desire to have more control over their personal information online (e.g., Gomez, Pinnick, & Soltani, 2009; Smit, Van Noort, & Voorveld, 2014; Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009). Consequently, personally managing and protecting online privacy has become an essential part of everyday life (Büchi, Just, & Latzer, 2017). (2018, 2)

What are students' thoughts regarding which entities (government, private sector, individual) should be responsible for it?

[53] As part of the debriefing part of the interview.

8.2.3.1 German Students

In an ideal world, Beate wants the EU to be responsible for a law regarding her privacy and data protection. She is an advocate for the new European GDPR law, as she thinks state laws are not beneficial to individuals who frequently move within Europe:

> It would be good if a state or a law — well actually not a state but Europe, because it doesn't make sense to have a state law with people moving around so much.
>
> *Dass es gut wäre, wenn ein Staat oder eine Gesetzgebung, nicht mal der Staat, sondern Europa in dem Fall, weil das wäre ein bisschen sinnlos, da Nationalgesetze dran zu binden, weil man so einfach oft Staaten wechselt ...*

Although later Beate says that:

> In any case, the government should be in charge of protecting privacy matters for its citizens. To be honest though, I don't think the government is actually doing it.
>
> *Der Staat [sich] drum [sic] kümmern sollte, auf alle Fälle die Bürger zu schützen auch. Ich habe mich aber schon sehr lange von dem Gedanken verabschiedet, dass das so ist.*

At the same time, Beate does not believe laws are enough to protect her personal information and data. She hopes that companies and app developers are fair, honest, and transparent. In her opinion, companies should be transparent when they use her personal information and data. She is slightly annoyed when a company such as Google lies:

> Well, like in recent times one notices Google is tracking one's location, even with one having the location service turned off. Well what a SURPRISE [laughing], well something like that, if Google, if they would tell you in advance, 'Look we are doing it for such and such reasons, maybe you won't understand them, but this is how we make money and improve our services.' I think then it is a fair and transparent deal as opposed to me wondering all the time, 'What is my smartphone doing [takes her smartphone into her hand] if it is turned off and what is it doing if it is turned on?
>
> *Auch jetzt gerade in der aktuellen Zeit, wo man gerade feststellt, oh Google checke deinen Standort, auch wenn du dein GPS mal nicht anhast. Na, ÜBERRASCHUNG [sie lacht], na eben sowas, dass dann halt auch Google das von vornherein auch klar gesagt wird, eh guck wir machen das aus dem und den Gründen, die vielleicht nicht immer nachvollziehbar sind, aber wir verdienen unser Geld damit und verbessern damit unseren Service, dann finde ich ist das eine faire transparentere Handel, als wenn man sich die ganze Zeit fragt, was macht mein Smartphone, wenn es halt nicht an ist [sie nimmt ihr Smartphone in die Hand] oder was macht es, wenn es halt an ist.*

Beate continues: "I [harbor] some distrust of certain apps and some mobile devices, but I don't think it has to be like that. There are apps I don't distrust." *("Das Mistrauen gegenüber manchen Apps, gegenüber manchen Geräten ist von Grund auf irgendwie da ist, dass, find ich, muss nicht unbedingt sein und da gibt es auch Apps, die das haben.")*

Jörg pauses and ponders for a bit before admitting that he finds my question difficult to answer. For him, the responsibility for protection should be shared by the government, companies, and the user. However, he emphasizes that, first and foremost, the government needs to establish laws and regulations and companies need to follow them. He does not think:

> Such cheap excuses, such as with the Facebook scandal, or with a lot of other cases, we didn't know about it or we weren't aware of it — well, that can't happen anymore. The [government] has to impose hefty fines, and it cannot be that these cases are in front of the court for years, as precedents setting, that is why you need the law.
>
> *Solche billigen Ausreden wie jetzt bei den Facebook Skandal oder bei ganz vielen anderen Sachen, von wegen haben wir nicht gewusst oder entzieht sich unsere Kenntnis darf nicht mehr ziehen, also, da muss es dann eben auch schon per gesetzlicher Grundlage eben empfindliche Strafen geben, das darf nicht jahrelang in Gerichtspräzedenzfällen noch hängen, dadurch braucht man eben die gesetzliche Grundlage.*

Nonetheless, he emphasizes:

> I am responsible for my own personal information and data. I mean, I have to keep track of what kind of apps I install, and how I link or interlink them, and I have to be conscious of what I release about myself, and as a person I have to know that even though, let's say, a company promises data protection of my data and is really thoughtful, I need to understand that systems are hackable. And then there is data trading – on purpose, that's why I believe all three entities [governments, companies, and oneself] need to work together, but then I believe the most important step is an up-to-date law, that's where one should start.
>
> *Ich selber bin natürlich auch verantwortlich für meine eigenen Daten. Also ich muss schon so ein bisschen den Überblick haben, was für Apps ich mir installiere, wie ich sie verknüpfe, und ich muss mir natürlich auch bewusst sein, was ich preisgebe, und ich mir als Person auch bewusst sein, selbst wenn eine Firma auf diese Daten sage ich mal aufpasst und sie sicher aufbewahrt, so ein System ist ja immer angreifbar. Es wird ja damit teilweise auch schon gedealt, das Daten abgegriffen werden, also da spielen alle drei zusammen, aber ich glaube, ein erster wichtiger Schritt ist vor allem eine aktuelle gesetzliche Grundlage, also da müsste man anfangen.*

8.2.3.2 American Students

Steve disagrees with the opinion of his German counterparts: He does not want the government to be in charge of mobile privacy protection because the government will harvest the information for its own good. He does not trust companies either, because their primary goal is to use one's data to make a profit. In his opinion, companies will find loopholes in order

to not protect their users' personal information. Therefore, Steve thinks that privacy protection is the responsibility of:

> Yourself, because basically governments will of course farm your information. They will find some way that they can farm your information for their personal use. Companies are primarily motivated by profit. So basically, if it costs them more money just to make sure that they can't spy on you, then they won't do it. But they will find some sort of loophole that says 'Hey, technically we protect your privacy but we still have to do this so we can get you the stuff that you like about us our site or our service.' So, it is up to us to make sure we don't do anything, we don't post anything, that we check what information is being shared on our apps and all that.

Yet, during the debriefing part of the interview, Steve retracts his opinion somewhat and now he is in favor of data privacy laws enacted by the US government to protect citizens' data privacy.

Ava disagrees, as she:

> … Think[s] the government should play a role in in it. Because I think just setting those standards helps. Sure, people can try to keep themselves to those standards and companies might have their own standards and that is okay, but people slip through the cracks otherwise and I think that, considering all the things that I heard about hacking and Russia trying to influence the United States election ...

She brings up how even her university, Rutgers, was the victim of large-scale hacking efforts. For her, "it is actually a national security thing, even your own personal device, so there should be at least some standard of security that the government should try to make people follow for companies and stuff. I don't think — I mean, I am for personal freedom but, in this case, some regulation would be a good idea."

Ava is not sure if the current administration is interested in enacting a federal data privacy and security law similar to the European GDPR.

> Do I think that the public, the people of the United States, which is what our government should come from, are interested in more security? I think that some are, but I think I am also biased because I am on the East Coast and I have a very liberal upbringing, and I know that the majority of Americans — maybe not the majority but a good deal of Americans — probably think that the government shouldn't have anything to do with their life, including their security.

8.2.4 Privacy Education

As Fieldwork 1 has shown, there are inconsistencies between mobile privacy attitudes and actual mobile privacy behavior. In the scholarly literature, this is called the "privacy paradox" (see also chapter 3.3 Privacy Paradox).
As one solution to the privacy paradox, several students suggested in Fieldwork 1 that there is a need for mobile privacy education. It is important to mention that none of the participants partaking in Fieldwork 1 and 2 had any data privacy and security instruction as part of their current or prior education.

8.2.4.1 German Students

The two German students share the same opinion – privacy education should start as early as possible.

Beate suggests that education should even begin before children have a chance to leave their digital fingerprints anywhere. She then compares privacy education to nutritional education and the ongoing debate surrounding it.

> To me, it is quite similar. Okay I admit it is a bit strange metaphor, but I compare it to nutrition. There is this ongoing debate about nutrition education, how to eat and cook, and then there is still no proper nutrition education in schools; not unless a teacher decides to do it voluntarily with his/her students. Moreover, I believe it is the same with data privacy stuff, and I would welcome it if kids were to be educated, because they are using these things [takes her phone in her hand].
>
> *Ich finde es halt so ähnlich, das ist jetzt eine komische Metapher, aber ich finde es, es passt ganz gut, wie Ernährung zum Beispiel. Man diskutiert seit Jahrzehnten darüber, wann soll man den Leuten was über Ernährung beibringen oder über die Grundbasis von Essen und Kochen und, wenn man es jetzt sieht, das ist immer noch nicht da, es gibt immer noch keine vernünftige Ernährungslehre, wenn da nicht mal ein Lehrer dabei ist, der sagt, ich mache es mit meinen Schülern mal. Und ich glaube, so ist es mit diesen data privacy [sic] Sachen, ich fände es total sinnvoll, wenn Kinder von klein auf, weil sie mit diesen Dingern halt in Kontakt kommen [sie nimmt ihr Handy in die Hand].*

In her opinion, there is a considerable need for children, teachers, and parents to be educated about privacy protections. "Oh well, if one talks about informatics or coding as part of the curriculum, then there should also be education about data privacy, which is similar to learning a language." *("Jaja, ich finde auch, dass das ein Teil von, wenn man schon von*

Informatik oder auch Programmieren spricht, als Unterrichtsfach unbedingt, dann finde ich gehört da auch auf alle Fälle Datenschutz.")

However, Beate also thinks that parents share some responsibility:

> And if parents allow their kids to use these things [mobile devices], then they have to be responsible at home, to teach their kids what it means to use these things. And I believe, well, I would say, [it] is a great idea to teach kids as early as possible and in a fun and approachable way about how these things work … My generation, born in the '90s, has a huge responsibility to teach their kids – it is a great thing, these mobile devices, [they are] super-useful, but one shouldn't assume it comes without a price.
>
> *Und, wenn Eltern entscheiden, ihre Kinder damit in Kontakt kommen zu lassen, dann haben sie auch dafür zu sorgen privat, dass ihre Kinder früh genug zu lernen, was es heißt, mit so einem Ding eine Verbindung einzugehen. Und ich glaube, da würde ich eher sagen, Schule ist eine gute Idee, so früh wie möglich, so spielerisch wie nur möglich, so einfach wie möglich zu erklären, wie das funktioniert … meine Generation, auch in den 90er Jahren geboren, hat da eine unfassbar große Verantwortung, ihren Kindern früh genug beizubringen, ist eine tolle Sache, kann alles sein Funktion haben, aber bilde dir nicht ein, dass das nichts kostet.*

Jörg's opinion complements Beate's:

> I believe one can start with digital stuff in primary school, and this could be [lessons like,] how do I use my smartphone in a mindful way, in order to not get addicted to it? How do I take breaks from it; how do I notice if I use it to procrastinate and such things? And I think that's when one should start with privacy stuff, too.
>
> *Aber ich glaube, man kann schon in der Grundschule mit so Digitalisierungssachen, also das kann ja schon sein, wie benütze ich mein Smartphone und wie schaffe ich es, gesund zu benutzen, dass ich nicht so abhängig werde, wie lege Ruhephasen ein, wie merke ich das mein Smartphone mich ablenkt, solche Geschichten und dann finde ich muss man mit den Privatsphären-Geschichten anfangen.*

Then Jörg remembers that he often sees young children using smartphones:

> I believe that I recently saw a child, maybe he was about nine, but come to think about it, in fifth or sixth grade, probably. Most kids have a smartphone, I am pretty sure, because for the parents it is also a safety net, it is really important for parents to be able to know where their kids are since they always know where they are and they can be reached via a phone call.
>
> *Ich dachte, ich hätte heute einen gesehen, der mag vielleicht auch neun gewesen sein, aber, wenn ich so überleg, fünfte oder sechste Klasse, da werden die ersten schon ihre Smartphones haben, da bin ich mir ziemlich sicher. Ich glaube auch gerade, weil den Eltern das mittlerweile sehr sehr wichtig ist, weil sie das Gefühl haben, ihr Kind ist auch sicherer unterwegs, sie können immer antworten, sie können telefonieren.*

In addition, he also thinks that primary schools should include information literacy as a mandatory subject.

> We have a lot at university about how to work academically, how to search and find information on a topic. Something like that should already be taught in primary school. Education is all about digital information literacy, and in such a course one could include data privacy and security.
>
> *Wir haben ja auch schon viel an der Uni wissenschaftliches Arbeiten, wie man recherchiert, sowas müsste es in der Grundschule auch schon geben, weil die Schulbildung ist ja heute sehr auf digitales Recherchieren ausgelegt, und genau in so einem Kurs kann man ja auch Datenschutz und Privatsphäre anbringen.*

Advocating for more awareness on privacy, Jörg emphasizes:

> I mean, one calls them digital natives, but they just take technology as a given without really being aware about stuff, not as aware as us being a bit older and thus we still remember the development … that's why I believe awareness is the most important thing. One cannot stop using these devices, one cannot take oneself out of the equation unless, of course, one becomes a hermit. And that's why you need the awareness of what is happening with one's information and data, and to be aware how exposed one is as smartphone user.
>
> *Ich glaube nämlich, man nennt sie alle immer digital natives, aber die benutzen die Technik nur, wie sie kommt, aber sie sind sich über viele Sachen gar nicht so bewusst, gar nicht so bewusst vielleicht wie wir, die ein bisschen älter sind und diese Entwicklung noch mitbekommen haben. Also ich glaube, da könnte man ganz schön ansetzen ... deswegen, denke ich, ist gerade das Bewusstsein das Wichtige, man kann ja gar nicht aufhören, man kann sich ja gar nicht so rausnehmen, außer man wird zum totalen Einsiedler und deswegen muss man sich einfach so, das benutze ich immer, bisschen Gedanken machen, das Bewusstsein darüber, was mit den Daten passiert, und einfach wissen, man ist jetzt offen an der Stelle.*

8.2.4.2 American participants

Both American students echo their German counterparts' sentiment: privacy education should already be part of the K-12 curriculum[54] with Steve commenting, "primary school because like kids are using the internet more and earlier and earlier … so, the sooner they understand that [the sites] they visit have consequences, the better. Honestly, I think the sooner the better because we all know that kids do stupid stuff all the time."

Ava adds, "I think, [with] how young people give their children smart technologies and phones I think that it should be done earlier and sooner rather than later, and it should be done in an

[54] US educators frequently use the terms K-12 education to refer to all primary and secondary education, from kindergarten prior to the first year (or 1st grade) of formal schooling, through secondary graduation (12th Grade) see https://isss.umn.edu/publications/USEducation/2.pdf

age-appropriate way." She continues, it "would be a good thing for students as young as elementary, middle, and definitely by high school to have some kind of education on security and knowing the type of dangers on the internet. There are some things you *should* be worried about and *should* know about."

Steve agrees that primary school children should learn about it and "… we need to warn them that, of course, some people are spying on you through your phone. What you do will affect you in the future … because I have seen so many careers ruined because of something they posted online a couple of years ago."
He suggests the curriculum should include education on privacy and security on your phone and computer as well as related topics such as cyberbullying. Steve believes that even though privacy education "won't fix the situation, at least [privacy education will] prevent some incidents [from] occurring."

Ava confesses that when she was young, she used websites or had a profile on social media sites even though she wasn't legally allowed to access these sites at that age:

> I know most websites don't allow you to create your own profile unless you are 14. Of course, they cannot really check this. When I was 14 I don't think I was allowed to create profiles. One of my favorite art websites, DeviantArt,[55] if you were underage you couldn't see more mature art, whether it is nudity or more sexual art. You couldn't look at it unless you were 18, but I just lied.

Concluding her thoughts on privacy education, Ava admits that she never had it as part of her curriculum:

> No, I am pretty sure … no, none of them did back in the day. If there was anything it was more like email etiquette and how to access university stuff. I didn't have anything like that back in high school. Maybe a teacher would say something unofficially, but it was never part of the curriculum. I didn't take communication [classes] or anything like that; they might say something at least in undergraduate about that. They do in the class that … I am going to be a TA [teacher assistant] for a class now, and they going to teach it.

[55] https://www.deviantart.com/

8.3 Mobile Security

Some participants brought up security or mobile security while talking about mobile privacy. Since this phenomenon is already observed in Fieldwork 1, this subchapter will briefly restate the findings on mobile security in Fieldwork 2.

8.3.1 German Students

Jörg brings up mobile security twice. First, he talks about security in relation to the Facebook scandal stating:

> Hmm … oh well, I was quite aware before it, in terms of security, but it confirmed my perception that all data and personal information, which are part of a deal in exchange for a free service — well, they really can be hacked. It doesn't matter how; if it's a professional cyberattack, or if it's because of carelessness, or one's own fault.
>
> *Hmm (…) Also ich hatte mir ja schon vorher ein relativ starkes Bild, glaube ich, auch gemacht, was Sicherheit an betrifft, und das hat mich in meinem Bild, glaube ich, auch nochmal bestätigt für mich selber, so dass ich dann gesehen habe, gerade die Daten die ja hinterlegt sind, mit denen man ja im Prinzip handelt und sich kostenlose Service erkauft, dass die wirklich teilweise angreifbar sind. Egal, von welcher Seite, ob das nun ein Hack ist, der professionell erfolgt, oder durch Unachtsamkeit oder eigenes.*

Jörg mentions it a second time when talking about being aware of what apps users install, as he cautiously declares, "a system can be always attacked or hacked. *("so ein System ist ja immer angreifbar.")*

8.3.2 American Students

Ava mentions security several times during the follow-up interviews. After being asked how she feels about mobile privacy following the Facebook scandal, she states, "But I think maybe the general awareness made me want to double check my security settings and who can see my stuff. I have it pretty secure anyway."

Regarding the new European privacy law, "I think there was kind of, there was something that passed about security protections legally." In terms of a data privacy law for the US, Ava reiterates her confusion between privacy and security while talking about a new law (see statement above).

8.4 Linguistic Highlights

This chapter presents linguistic highlights organized by participant. Emphasis is given to words, phrases, and nonverbal cues that best portray participants' sentiments about mobile privacy.

8.4.1 German Students

During the interview Beate used the following expressions:

*.. **Verarschen kann** ich mich auch selber [sie lacht laut], also ich habe ein Pakt mit dem Teufel geschlossen.*	**My ass,** [she laughs out loud], I mean I have a pact with the devil.
*Dieser **Kuhhandel oder dieser Handel mit dem Teufel quasi.***	the **horse trading or the deal with the devi**l.
*Also, wenn man mal ehrlich ist, das Gesetz ist ja eine nette Idee, **aber das ist so lückenhaft und schwachsinnig**, das eigentlich." Das er total verstehen kann das sich so viele Leute eine neue Datenschutzverordnung zulegen, aber so richtig helfen tut es auch nicht." Es ändert nicht wirklich was meinte er dann.* *Na **ÜBERRASCHUNG [sie lacht],** na eben sowas, dass dann halt auch Google das von vornherein auch klar sagt.*	To be honest, the law it is a nice idea, **but it's patchy and really stupid.** He [her roommates' boyfriend – a lawyer] really can understand why people have to have a new data privacy policy, "but it doesn't really help. it won't change anything" – that's what he said. **SURPRISE [she is laughing]** Oh, wow, if Google would be open, honest from the start, the get-go.
*Ja **dieses Scheinheilige,** ja*	**it is hypocritical**
BOA!!** Ob ich welche erhalten habe Mir war gar nicht klar wie viele Konten ich habe. **[Sie lacht.]	**Phew,** I got a lot, I didn't even know how many accounts I have. [**laughing]**
*Ja, da waren bestimmt so fünf oder sechs Stück dabei, wo ich dachte "**Oh da habe ich ein Konto." [Sie lacht]***	I mean maybe for five or six accounts I thought, "**really, I have an account there?" [laughing]**

Jörg's language includes the following expressions:

*Und da war ich schon **ziemlich stinkig, da habe ich mich nämlich genötigt gefühlt**, mein Profilbild zu ändern und mein Status.*	I mean **I was pissed, because I felt forced** to change my profile picture and my status.
*... immer noch weltweit die Mentalität, einfach irgendwas unter **den Teppich zu kehren.** Man hört und liest auf Foren, wenn wirklich mal **richtig Scheiße gebaut** wird, ist die erste Reaktion nicht, wie gehen wir jetzt damit um, wie machen wir das jetzt allen klar, dass wir Mist gemacht haben, sondern die erste Reaktion ist immer, wie können wir das verschwinden lassen.*	… worldwide the mentality is **to sweep it under the rug,** I hear and read in forums, if **a fuck-up happens,** the first reaction usually is not how do we deal with it?, no, the first reaction is how can we make it disappear?
*...Also solche **billigen Ausreden***	... And such **cheap excuses**

8.4.2 American Students

Here is a selection of Steve's statements:

> Even though you **kind of DO know** it in the back of your mind that they doing it, but of course now that it is official **everybody is getting upset**.
>
> It felt, it certainly **didn't feel any good**. It basically just made me **fearful** of what I kind of post on my phone. Even so I try not to do anything of course bad on it.
>
> Well **[sighs somewhat]**, no not really because I at this point **if I did anything bad, they already know about it**. But other than that, it is basically I DO try to keep conscious of what sites I visit, what I click on.

Ava's vocabulary encompasses the following:

> I mean, I knew after our conversation that things were kind of tracking me or that they kind of **trick you** in mobile devices to get more information on you.
>
> Or I logged in with something and deleted the app and who knows **who's got the data? [laughing] that is kind of scary [laughing]**.

8.5 Summary

In this chapter participants opinions on the Facebook data breach scandal have been described. Following student's awareness, and perception about the new European data privacy law (GDPR) as well as opinions on privacy education and privacy protection have been depicted. Mobile security and highlighted linguistic expressions concluded this chapter.

9. Discussion Fieldwork 1

9.1 Overview

The following chapter discusses the most striking findings from Fieldwork 1. For each topic, first, any similarities between both cultures will be discussed. Then, if there are any unique findings, these are debated. Each topic includes a cultural summary, with a focus on the possible difference between mobile privacy behavior and attitude for each culture. Furthermore, since language plays an integral part in this cross-cultural study, the linguistic highlights are deliberated. As noted in the introduction, the first-person voice is used to present the ethnographers' opinion.

9.2 Themes

9.2.1 Mobile Phone Behavior

9.2.1.1 Similar Aspects between German and American Students

Much has been written on smartphone addiction (see, for example, Jones 2014; Davazdahemami, Hammer, and Soror 2016; Lopez-Fernandez et al. 2017).
Shambare, Rugimbana, and Zhowa (2012) even go so far as to proclaim that "mobile phone usage is not only habit-forming, but it is also addictive; possibly the biggest non-drug addiction of the 21st century" (573). The composite narrative also shows that in both countries, participants use their smartphones in similar manners. One interesting association founding both groups was that even the "late phone adopters" (nine participants – see chapter 5 Quantitative Data) quickly became accustomed to their smartphones. Many of them quickly developed habit-forming behaviors such as using their phone as an alarm clock. However, in both cultures, what I call mindful smartphone usage also emerged. For example, students use it less if they are spending time with friends. This shows that even though the students (and I would not exclude myself here either) certainly use their phones a lot, they also value social interactions and spending time without being connected.

Clearly, these findings are transferrable and reinforce what is already known and has been researched in the scholarly literature for some time now: smartphones are ubiquitous among young adults. Taylor and Silver confirm it by stating:

> Whether, in advanced or emerging economies, younger people, those with higher levels of education and those with higher incomes are more likely to be digitally connected.[1,2] Younger people in every country[56] surveyed are much more likely to have smartphones, access the internet, and use social media. (Taylor and Silver 2019, 4)

9.2.1.2 Cultural Comparative Summary

When it comes to participants' phone habits and behavior, there are many similarities. One slight difference is in the usage of messenger apps for German students, which I address specifically in subchapter 9.2.6 WhatsApp. Undoubtedly, there are some differences regarding what *kind* of apps are most popular within the investigated cultures, but this is beyond the scope of this study. I defer to other scholars such as Lopez-Fernandez et al. (2017), Yang, Asbury, and Griffiths (2019), Lee and Song (2015), and Lim et al. (2015).

9.2.2 Mobile Phone Attitude

9.2.2.1 Unique Aspects of German Students

The four distinct findings regarding mobile phone attitudes and behaviors among German students are:

- None of the German participants owned an Apple iPhone and instead had phones running some form of Android mobile operating system (mOS/mOS). This is not surprising, as statistics confirm that Android is the leading mOS among Germans, with 78% using Android mOS compared to 20% using Apple iOS as of the first quarter of 2019. (*Smartphone OS: Sales Market Share in Germany 2019* 2020, 10).
- A positive attitude about having an open-source mobile operating system installed on the phone; this was considered by some participants to be superior to the "regular Android." None of the US students who use Android mention this specifically, but two German students emphasize how CyanogenMod offers excellent privacy features.
- Value for money is another unique finding among German students**.** Price is undoubtedly the ultimate deciding factor in how they choose and purchase a new smartphone.

[56] such as South Africa, Brazil, Kenya, India, South Korea, France, Germany, and the US.

- German students do not express any need for the newest gadget, nor the "cool" Apple iPhone (see in contrast the American participants' attitude below)

These two findings (concerns about value, but not necessarily about having the newest gadget) correspond with two statistics where:

The likeability of Apple's iPhones and Samsung Galaxy (Android):

29,56% find the Apple iPhone likable versus
38,40% who find Samsung Galaxy likable.
(*Smartphones in Germany* 2019, 39,49)

Quality perception of Apple's iPhones and Samsung Galaxy (Android):

38,57% for the Apple iPhone versus
39,64% for Samsung Galaxy. (*Smartphones in Germany* 2019, 49)

Moreover, I correlate this to Hofstede's dimension of indulgence (see also chapter 3. Literature Review): "The low score of 40 on this dimension indicates that the German culture is restrained in nature." (*Country Comparison Germany and USA* 2019). It might be that German students have less need for self-indulgences, and therefore owning an Apple iPhone, which I consider a luxury smartphone, is of less importance. I would also argue that displaying one's wealth is somewhat frowned upon within German society, and therefore an Apple iPhone is less likely perceived as a status symbol for German students.

German participants showcase specific attitudes regarding messenger apps, such as Threema or WhatsApp. I will discuss this in greater detail in subchapter 9.2.6 WhatsApp.

9.2.2.2 Unique Aspects of American Students

Most of the US students owned an Apple iPhone, and several students, including the late adopters, were adamant about purchasing an iPhone. According to Schmuck, Kasser, and Ryan (2000, 4), "the U.S. is generally a very consumeristic culture in terms of its exposure to advertising and the myths suggesting that wealth and status are highly important (Astin, 1998; Murphy and Miller, 1997) …" (2000, 4). It is interesting to observe that the relatively high price did not seem to have any impact on the participants' decision to have or purchase an iPhone. After all, these are presumably students with limited income, and in the U.S., university education is not free. However, even though Rutgers is a state university, it is a relatively elite university: "median family income of a student from Rutgers is $103,500, and 47% come from

the top 20 percent" (Aisch et al. 2017, para. 3). In comparison to Lehman College, The City University of New York, the University where I worked for several years, the median family income was "$41,652 per year, and 72% of students can be considered low-income as indicated by their receipt of Federal Pell Grant Aid." (CollegeSimply n.d., para. 5)

Nonetheless, this finding confirms a survey of American consumer's preferred smartphone brand. As of March 2019, Apple's iPhone has a 46%, market share with the remaining 54% distributed to:

30%	Samsung	2%	Google
10%	LG	1%	Huawei
4%	Motorola	1%	HTC
3%	ZTE	2%	others ("Smartphones in U.S." 2018, 25)

Thus, American students might justify the purchase of a more expensive phone because owning an Apple iPhone is not necessarily considered a luxury.

9.2.2.3 Cultural Comparative Summary

There are clearly some cultural differences between the two study groups. I can only speculate whether these differences have any impact on participants' mobile privacy behavior and mobile privacy attitude. For example, if Aldi (a discount supermarket) started selling Apple iPhones cheaply in Germany, would students then buy an iPhone? Alternatively, if an independent company started selling pro-privacy cellphones with a premium price that did not run on either Android or iOS, would German students invest in these?

Overall it remains unclear to me whether the portrayed differences in mobile phone attitudes have a real impact on mobile privacy behavior and attitude. I cautiously would say no, but I admit further research had to be done to come to a valid conclusion.

9.2.3 Privacy Definition

9.2.3.1 Similar Aspects German and American Students

Both the German and American students find it equally challenging to explain privacy from an abstract as well as a personal point of view.

This result was to be expected, since privacy is a vast, complex topic. Not only do non-experts find it difficult to define, but as the literature review chapter (see 3.2 Privacy Concepts and Definitions) has shown, it is a difficult concept to delineate for privacy scholars from all kinds of disciplines (see Benjamin 2017; Bélanger and Crossler 2011). This finding also resonates with what Sigmund asserts: "[up] till now we do not have a detailed enough definition of privacy. 'Privacy [...] is a concept in disarray. Nobody can articulate what it means." (Solove, 2008, p. ¡) This idea articulates how difficult it is to unanimously agree upon a definition of privacy" (2017, 37). Herein lies a fundamental issue: if scholars cannot agree or articulate privacy in a succinct, comprehensible, and applicable fashion, it is understandable that research participants struggle with it.

Another illuminating discovery from the study was students in both cultures associates the loss of privacy with some sort of harm or danger — be it identity theft, financial damage, stalking, or burglary. Interestingly, the physical loss of privacy, e.g., burglary or stalking, seems to be perceived by some participants to be more severe than the more abstract loss of identity theft. This finding is consistent with the finding that privacy "risks with a physical safety component (stalking, burglary) are perceived to be most severe." (Gerber, Reinheimer, and Volkamer 2019, 279)

Nearly all students connect privacy primarily to the digital realm, the world of apps, websites, and social networks. Two possible reasons: First, most research participants grew up with the internet, computers, and mobile devices as a part of everyday life and are therefore digital natives. And second, because of the study's topic, participants may have been more attuned to the digital and mobile aspects of the topic.

9.2.3.2 Unique Aspects of American Students

An unexpected result was how much value the American student groups associate with privacy. I had anticipated more responses along the lines of "privacy is dead" or "transparency

is the new privacy." However, the finding in this study supports what quantitative research article by Hoofnagle et al. (2010) discovered:

> In policy circles, it has become almost a cliché to claim that young people do not care about privacy. Certainly, many troubling anecdotes are surrounding young individuals' use of the internet and social networking sites in particular. Nevertheless, we found that in large proportions, young adults do care about privacy. (2010, 20)

Moreover, this finding also contradicts my previous belief that young adult American students do not value privacy. It is also supported by my personal and professional experiences over the last few years, as I have seen something of a shift within American students' attitudes — and even the public at large — when it comes to privacy. I theorize this might be due to the public and media attention the Facebook data breach received. Moreover, the new European data privacy law (GDPR) has received quite a bit of attention in the U.S., too, and maybe this has had a positive impact.

Yerukhimovich et al. support this by arguing in 2016:

> Americans desire privacy, as demonstrated by several recent polls conducted by the Pew Research Center (Boyles, Smith, and Madden, 2012; and Madden and Rainie, 2015). A majority of Americans surveyed have avoided using one or more smartphone apps because of privacy concerns. Many people say that it is important to be in control of access to their private data and do not want people watching them without permission (Boyles, Smith, and Madden, 2012; and Madden and Rainie, 2015) (2016, 2).

9.2.3.3 Cultural Comparative Summary

All students share some common dominators regarding the definition of privacy:

- the right to be left alone, to have secrets and remain anonymous;
- the ability to decide what personal information they want to disclose to whom and when;
- the ability to control and have a choice of what, how, or if they disclose personal information and data.

All participants perceive their personal information as the most valuable part of maintaining privacy. Interestingly students' definitions of privacy have many similarities with descriptions reviewed in the literature chapter three dating back to pre- or early days of computer technology such as Westin (1967) and Ware (1977).

Overall, there were few differences between the two cultures' definition of privacy.

9.2.4 Mobile Privacy Definition

9.2.4.1 Similar Aspects between German and American Students

Overall, the majority of students do not think that mobile privacy is even possible. This finding exemplifies an attitude I call **mobile privacy learned helplessness** in this study I define it as the feeling of being unable to have control of one's mobile privacy.

To my knowledge, associating smartphone behavior and attitude with learned helplessness has only been described by Shklovski et al. in 2014. They state that "learned helplessness typically happens when people come to believe that a situation is unchangeable or inescapable." (2014, 2354) However, the term itself, and even the establishment of a learned helplessness theory, has been identified by the American psychologist Martin Seligman in the late '60s and early '70s. (Nolen 2019):

> Learned helplessness, the failure to escape shock induced by uncontrollable aversive events, was discovered half a century ago. Seligman and Maier (1967) theorized that animals learned that outcomes were independent of their responses—that nothing they did mattered—and that this learning undermined trying to escape. (Maier and Seligman 2016, 349)

Later, the theory of learned helplessness was observed and used to describe human behavior, linking it, for example, to depression or child development issues. (Mohanty, Kumar Pradhan, and Kesari Jena 2015, 886). I admit that the term "learned helplessness" certainly carries an undertone of despair that some might consider too stark to be linked to mobile privacy.
Even if a smartphone user has the autonomy or ability to control her privacy settings on the device, it seems pointless to do anything about it. It is intertwined with both the attitude and the behavior and, as such, might also be a better explanation than what many researchers define as the privacy paradox, which is the discrepancy between privacy attitudes and actual privacy behavior. While I certainly discover the existences of the privacy paradox, I do agree with what Shklovski et al. assert: "the implication here is that perhaps there are other explanations for what has been termed the privacy paradox [36], beyond decision making conundrums and situational constraints." (Shklovski et al., 2354) My claim is also relatable to what Choi, Park, and Jung (2018) define as privacy fatigue: "frequent data breaches remind

people that they are not in control of their online information. Privacy fatigue reflects a sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet (Acquisti, Friedman, & Telang, 2006; Hargittai & Marwick, 2016)." (2018, 41). The authors' definition is very similar to what I call mobile privacy learned helplessness, yet the most important association toward my points is their assertation that:

> The findings in this study imply that the concept of privacy fatigue can be used to explain the discrepancy between individuals' attitudes and behaviors known as the "privacy paradox"– the phenomenon that consumers disclose personal information despite their privacy concerns (Barnes, 2006; Norberg, Horne, & Horne, 2007) …Therefore, privacy fatigue can provide a possible rationale to explain the discrepancy of why individuals intend to disclose their information, despite having high levels of privacy concerns. (2018, 49)

9.2.4.2 Unique Aspects of German Students

It was somewhat easier for German students to define mobile privacy. One reason could be that the German research participants of this overt study have some prior interest or knowledge —through their education, social milieu, and media — about the topic. And referring back to the literature chapter (see Privacy and Data Protection History) Germany's troubled history, in which privacy was repeatedly trampled on, may continue to affect current citizens' feelings toward privacy.

9.2.4.3 Unique Aspects of American students

I observed in the American participants more pauses, vocal hesitations, and uncertainty when asked about mobile privacy. It is possible that the terminology itself is relatively new and, therefore, more like jargon used by scholars and has therefore not entered the everyday U.S. lexicon. To be fair, after I explained the question in greater detail, many American participants were able to come up with insightful and thoughtful answers. Therefore, this does not delineate American students' ignorance of mobile privacy as a concept; they simply might not be as familiar with the term itself.

9.2.4.4 Cultural Comparative Summary

Both groups had a somewhat harder time grasping the different between mobile privacy and privacy. Which I presume is due to the fact that a) mobile privacy is a relatively new research area and b) many articles reviewed in the literature subchapter on mobile privacy do not come up with their own particular definition but instead refer back to prominent scholars such as Westin (1967), Altman (1975), Ware (1977) and Nissenbaum (2010).
Hartmann (see also literature review chapter 3.9. Mobile Privacy) acknowledges this by stating the "combination of privacy and mobility is potentially problematic," and she perceives it as "helpful in defining mobile privacy and to explaining its meaning further" by looking at "first perspective deals with technological research, the second with a philosophical approach to the contexts of privacy." (2011, 192)

Nevertheless, in terms of cultural comparison, there was no significant difference between participants' attitudes when defining mobile privacy.

9.2.5 Mobile Privacy User Behavior and Mobile Privacy Attitude

9.2.5.1 Mobile Privacy Setting Behavior and Attitude

9.2.5.1.1 Similar Aspects between German and American Students

Comparing American and German students' mobile privacy setting knowledge and behavior, both user groups span a wide field of competency.
I divide their competency into three different types:

Type 1 Students exhibiting
proactive and knowledgeable mobile privacy behavior and/or attitude

Type 2 Students exhibiting
moderate knowledgeable mobile privacy behavior and/or attitude

Type 3 Students somewhat
indifferent or confused by complicated privacy settings on their smartphones

Type 3, the indifferent users, displayed a complacent mobile privacy behavior and attitude, which some of the moderately proactive mobile privacy users (Type 2) also represent at times. The Cambridge English Dictionary defines complacency as "a feeling of calm satisfaction with

your abilities or situation that prevents you from trying harder." (*Complacency | Definition in the Cambridge English Dictionary* n.d.)

After all this research and my experiences, I understand **mobile privacy complacency** as accepting of the current status quo, in terms of an attitude as well as/or behavior. In my understanding, it also includes a bit of arrogance. I see it related to mobile privacy learned helplessness, but identify it as a bit less pronounced and a bit milder.

After trying to find comparable and transferable previous research, very little was found in the literature on mobile privacy setting management. To date, only Park and Mo Jang (2014), as well as Baruh, Secinti, and Cemalcilar (2017), specifically researched it. Park and Mo Jang used quantitative and qualitative methods to "put forth a new measure of digital literacy that focuses on mobile privacy-related skills and knowledge. Here the notion of mobile privacy literacy describes specific knowledge and skill regarding privacy-related functions in the mobile phone." (2014, 297). While their study was limited in terms of its participants (African American young adults only), some of their qualitative findings correlate to my results. For example, in regard to being confused about privacy setting features, a 24-year-old African American male BlackBerry user who worked for a local delivery service commented:

> 'Oh yes, I use my BlackBerry all the time. Um, this is here. Maybe, too many options and keys ... If I don't pay attention to them, let's say it is really something new, yes I would not know [privacy options] as a part of those settings until maybe I got to know them later or didn't feel like okay. I don't feel comfortable to share my personal life with them. I may take them out, but initially, they were new to me, yea, I definitely would not know.' (Park and Mo Jang 2014, 301)

I recognize a similarity in what (Park and Mo Jang 2014) declare as a significant finding, as they "are concerned that a relatively high level of mobile familiarity did not translate into mobile privacy knowledge". (2014, 302) This study observed mobile privacy setting behavior and attitude. All participating students portrayed a high level of mobile familiarity, but this is not an indicator of how well they understand the mobile privacy settings on their phones.

Another notable finding in both cultures is a very similar behavior and attitude about location service features. The three aforementioned different behavior types (Type 1 very proactive to Type 2 moderate mobile privacy behavior) are applicable here again. I address location service attitude separately, later in this discussion.

The last exciting finding concerning privacy setting behavior and attitude is participants' confusion between privacy and security. I will discuss this phenomenon further in subchapter Mobile Security Behavior and Attitude.

9.2.5.1.2 Unique Aspects of American Students

One behavior unique to the U.S. students is that they all openly self-acknowledged and self-reported not using their mobile privacy settings features very often. This admission might be because the trust and the rapport between researcher and interviewees is excellent and, as such, they feel comfortable in voicing their honest opinions. I also speculate this could be due to what I have defined previously as "mobile privacy complacency attitude and behavior" and, perhaps to some degree, mobile privacy learned helplessness.

9.2.5.1.3 Cultural Comparative Summary

An interesting correlation between Baruh, Secinti, and Cemalcilar (2017) meta-review and this study is their claim that:

> Specifically, the indulgence/restraint dimension focuses on cultural differences related to the balance between satisfaction of needs (in this context, e.g., self-presentation) and social norms (such as those related to privacy). Our moderation analyses indicate that the results discussed above can be generalized across cultures that differ from each other in terms of indulgence/restraint orientation and level of legal protection for privacy. This finding needs to be interpreted in light of research suggesting that despite cultural differences in usage patterns associated with Internet use (e.g. Li&Kirkup, 2007), there are also significant overlaps across cultural contexts … (2017, 47)

I certainly agree with this statement about both cultures – the US and the German differ not only in their legal protection, but have a significant difference between their indulgence/restraint dimension. Germany has a moderate indulgence dimension of 40 %, which can be translated to the "mentality of 'work hard, not play'" (Yang et al. 2016, 62). For the US, the indulgence dimension is higher, with 68%. Furthermore I would like to bring back an interesting finding from the literature chapter, which Trepte and Masur (2016) claim that American and German's self-evaluation about their privacy literacy ability is higher as

compared to, for example China, the Netherlands or the United Kingdom (see chapter 3 Multinational Research, page 22)

In summation I do not see cultural dissimilarities in participants' behavior and knowledge on managing their mobile privacy settings. The similarities outweigh the differences.

9.2.5.2 Location Service Attitude

9.2.5.2.1 Similar Aspects between German and American Students

All research participants portray an attitude hostile to constant surveillance and personal information sharing via locating tracking. I speculate this is because location tracking, privacy, and smartphones have been researched in the scholarly literature (see Barkhuus and Dey 2003; Fisher, Dorner, and Wagner 2012; Almuhimedi et al. 2015) for quite some time. Additionally, in recent years, mainstream media has reported about it frequently (see Warren 2013; Beres 2014; Mims 2018). I claim this has raised awareness about location tracking, and education might have had a positive impact on participants' perceptions. Additionally, over the years, mobile operating systems have made it easier[57] to control location tracking on smartphones and apps. Indeed, this study's research participants are well aware of how location tracking works, and, their behavior and attitude reflect this. The findings in this study confirm that in "recent literature review that people's views on location privacy have changed over time: early studies (before 2010) show little concern for location privacy, but more recent studies show otherwise …" (2019, 2). It seems that participants value the control they may or may not have to protect their location privacy. Furthermore, this also shows that people know how to use or not use location tracking. The combination of improved usability in location settings and improved knowledge education seems to be correlated to the attitude and also then the behavior of this study's participants. This leads me to the assumption that if people have the option of keeping their mobile location private, and it is perceived as relatively easy and hassle-free, this studies participants' do protect it. Yet I do not have enough evidence whether this also could lead eliminating or reducing the privacy paradox.

Additionally, trusting an app or app developer seems to be correlated to location privacy attitude not only in this study's findings, but also in…:

[57] For iPhone with iOS 8 in September 2014: https://support.apple.com/en-us/HT203033
and for Android https://support.google.com/nexus/answer/3467281?hl=en

> Users behave in a manner that is consistent with them desiring varying amounts of location privacy. Some apps are more trusted than others with location data. Knowing past decisions by a user or by other users about a particular app can inform whether a particular user will grant location access to a particular app. (Fisher, Dorner, and Wagner 2012, 55)

9.2.5.2.2 Unique Aspects of German Students

Only the German participants admit confusion, ignorance, and or belief in a lack of transparency about the flow of location data. A recent study by Brandtzaeg, Pultier, and Moen (2018) confirmed that:

> Many apps lack transparency about how they will use personal information (Sunyaev, Dehling, Taylor, & Mandl 2015). Many apps also request and share detailed user information without justifying the data collection and sharing process. For example, recently, it was revealed that the gay-dating app Grindr shared HIV-testing and location data with two third-party players (Ghorayshi & Ray, 2018). (2018, 467)

Another possible explanation of why German students' show these unique findings could be that the Android mobile operating system location tracking notification differs from that of an Apple iPhone. As a test, I downloaded the running tracking app Adidas Laufen und Fitness Runtastic[58] on an Android[59] from the German Google Play Store and Adidas Running app Runtastic[60] on an iPhone[61].

Figure 21 + 22 shows location tracking notifications after installation and first-time activation of the app.

[58] https://play.google.com/store/apps/details?id=com.runtastic.android&hl=de

[59] On January 23, 2020 using Android 7.1.1

[60] https://apps.apple.com/us/app/adidas-running-app-runtastic/id336599882

[61] On January 23, 2020 with iOS version 13.3.1

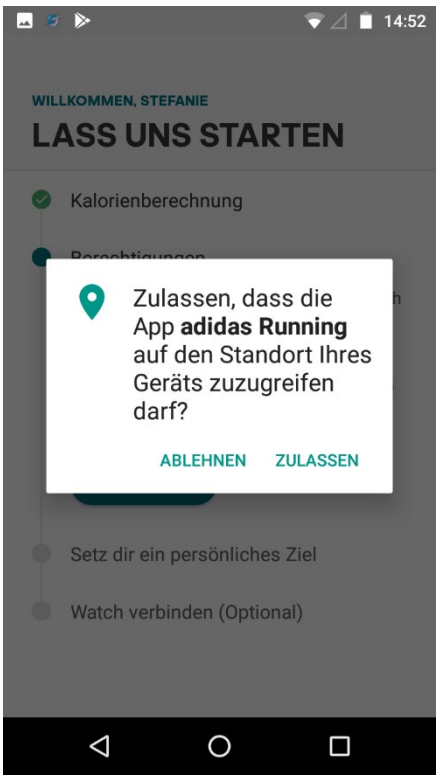

Figure 20 Screenshot of Fitness Runtastic app on Android
"Allow adidas Running to access device location … Deny – Accept"

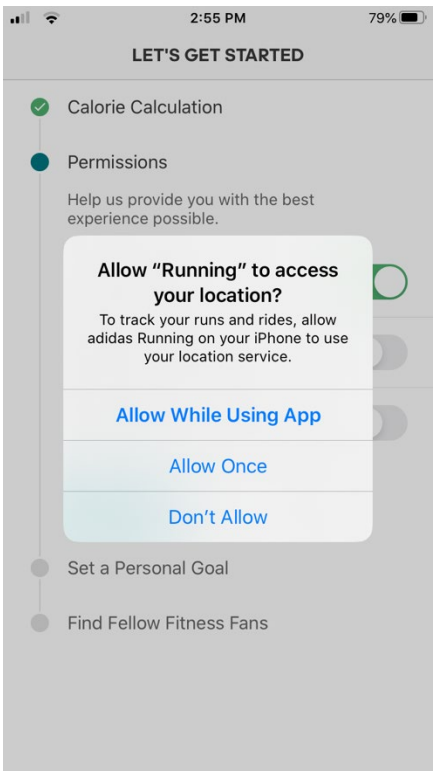

Figure 21 Screenshot of Fitness Runtastic app on Apple iPhone "Allow "Running" to access your location? To track your runs and rides, allow adidas Running on your iPhone to use your location service. Allow While Using App. Allow Once. Don't Allow.

I find the pop-up notification on the Apple iPhone (see on the right side) to be more transparent in the language. Moreover, the iPhone has three different options to choose from, whereas the Android (on the left side) only gives you one option to control location tracking.

9.2.5.2.3 Cultural Comparative Summary

When it comes to participants' opinions on location service I cautiously claim that there are no cultural differences. Furthermore, when linking mobile privacy behavior and attitude to location service I also think Nissenbaum's framework of contextual integrity for privacy could be an explanation, in that "privacy may be still posited as an important human right or value worth protecting … but what this amounts to is a right to contextual integrity" (Nissenbaum 2010, 127), which:

> Articulates a model wherein informational norms are defined by three key parameters: information types, actors, and transmission principles. It postulates that whether a particular flow, or transmission of information from one party to another is appropriate depends on these three parameters, namely, the type of information in question, about whom it is, by whom and to whom it is transmitted, and conditions or constraints under which this transmission takes place. Asserting that informational norms are context relative, or context-specific, means that within the model of a differentiated social world, they cluster around and function according to coherent but distinct social contexts. (Nissenbaum 2018, 839).

This may explain the students' location service attitude in as much it might be deemed acceptable for Google Maps or geotagging on Snapchat, but inappropriate for a music app like Perfect Piano (see also results in the following subchapter).

9.2.5.3 App Experiment Perfect Piano Behavior and Attitude

9.2.5.3.1 Similar Aspects German and American Students

The following similarities between German and US participants were uncovered during the interview stage.

Before downloading the app, none of the participants looked for, much less read, the privacy policy, which is included in the Apple App Store or Google Play Store. This finding is comparable to several prior studies (see for example, Aïmeur, Lawani, and Dalkir 2016; Ermakova et al. 2014) on privacy policy behavior on desktops and apps, with Chin, et al. (2012), declaring:

> End user agreements, privacy policies, and terms of agreement are explicit security and privacy indicators. Few participants consider them before installing mobile phone applications, which is consistent with past literature [16, 6]. Surprisingly, 60% of participants with Android phones report 'Sometimes' or 'Always' considering permissions, although it is one of the lowest-ranked factors. These results indicate that participants rely on other indicators of trust (e.g., recommendations and reviews) instead of these explicit but hard-to-understand security and privacy indicators. (2012, 9)

On both stores' interfaces, the privacy policies of apps could be described as somewhat hidden. In fact, in the time since the interviews were concluded, Google Play Store has redesigned its layout, and the privacy policies are even more challenging to locate. To find the privacy policies in both stores, one has to scroll down nearly to the end of one's phone display

on the Apple iPhone, and on Google Play, one even has to go a step further and click. Scrolling as a navigation option, is not recommended by Harms et al.:

> Scrolling performed worst in all of these measures. The remaining three patterns worked equally well. Qualitative results and subjective rankings provided the explanation that the more interactive patterns (i.e., Tabs, Menus, and Collapsible Fieldsets) offer a better overview than Scrolling. We conclude that designers should avoid Scrolling in favor of the other patterns …. (2015, 339)

I also hypothesize that the official app stores, which are operated by Apple and Google, do not want customers to find the privacy policies easily. Even though they both claim that they care about user's mobile privacy,[62] the design presents a different picture. If one cannot find a privacy policy, one cannot read it, and therefore, as a user, one remains unaware of any possible mobile privacy infringements. Both app stores could redesign their layouts to better draw attention to relevant privacy policies.

Instead of reviewing relevant privacy policies, many participants relied on the star ratings and reviews included in both app stores. A recent study by Joeckel, Dogruel, and Bowman (2017) between the same cultures investigated in this research confirm cultural similarities as:

> Eleven German and 11 U.S. participants mentioned ratings or reviews as a salient cue for deciding which flashlight to use. Good ratings and reviews seem to be sufficient to decide which app to download: 'The one that had the better review, so that was the one I picked' (U_M_9), or to put it very simply: 'I chose that one because, well it has five stars and I mean I know the other ones have five stars too, but usually I just choose the first one' (U_F_13). (2017, 629)

And according to Stoyanov et al. (2015) there is:

> Little information on the quality of apps available, beyond the star ratings published on retailers' Web pages, and app reviews are subjective by nature and may come from suspicious sources [6]. Selecting apps on the basis of popularity yields little or no meaningful information on app quality [7]. (Stoyanov et al. 2015, 2)

Even though several other rating systems for apps exist, from both private as well as academic sectors,[63] there is not universal gold standards for ratings or certified option available for users to obtain information about an app and its privacy behavior. One solution brought

[62] For Apple see for example https://www.youtube.com/watch?v=Py0acqg1oKc and https://www.apple.com/privacy/
For Google see https://developer.android.com/privacy and https://safety.google/privacy/privacy-controls/

[63] See for example http://privacygrade.org/ or https://mhealth.jmir.org/2015/1/e27/

forward by Arzola and Havelka (2016) is for librarians to become more involved in the evaluation of apps:

> Librarians rely on assessed resources to work smarter, as well as introduce these resources to students. App evaluation is necessary to identify reliable, relevant, up-to-date, intuitive apps that support students' research needs, as well as respond to curriculum requirements. Therefore, evaluating authoritative apps help students make responsible choices. (2016, 55)

The last similarity is that most of the Android users seem to be more careful about allowing and not allowing permission (either by reviewing permissions before installation or while using the app). I will address this further in the cultural comparison of this subchapter.

9.2.5.3.2 Unique Aspects of American Students

None of the American students tried to go into the privacy settings menu after the installation of the app to verify or modify the apps privacy settings. This fits into what I discussed previously about student's non-usage of their phone privacy settings. Again, as above, I correlate this to mobile privacy complacency behavior and attitude. Additionally, trust might be another explanation. The rapport I shared with the students was excellent, and, as such, students trusted that I would not to ask them to download an app that would infringe on their privacy.

Furthermore, other research has shown that:

> App marketplaces were highly successful in transferring trust from their well-known brands – Android App Market, Amazon's marketplace, Apple's iTunes, and the Apple App Store – to their affiliates and partners. For example, if participants were using an app on their mobile device for shopping, regardless of which company made the individual app, because the app had been approved through a larger trusted company (e.g., Apple), the trust the participant had with that company transferred to the app itself. A similar phenomenon occurred for purchasing or downloading apps themselves. Because apps were approved by a larger, trusted company, apps themselves were considered to be trustworthy. (Hillman and Neustaedter 2017, 14–15)

One last distinction among American students that I would like to discuss is how none of the students allowed notifications for the Perfect Piano app.

All of the American students denied push notifications for the Perfect Piano app. I speculate this might be due to the fact that the students do not see the value in allowing a game app to

send notifications, and that they might allow them if the app was, for example, a messenger app.

Here Nissenbaum's theory of context integrity again offers a possible explanation, as " control over information is an important transmission principle, but always with respect to particular actors and particular information types, all specified against the backdrop of a particular social context" (Nissenbaum 2018, 840).

Hence, I am wondering if the American Apple iPhone user would allow an app similar to the one described in the above quote to send them regular notifications or if quite contrary it would lead to mobile privacy complacency and participants would deny notification from the beginning or at a later point for such an app?

9.2.5.3.3 Cultural Comparative Summary

Above I hypothesize whether there is a possible association between Apple iPhone user's mobile privacy behavior/attitude and Androids. I could not find a lot of studies on this topic, however, an online survey with German participants discovered that:

> Significantly, more Android users stated in an open-ended question that privacy issues and permissions are important for them when deciding to install a new app (see Fig. 1(b)). They did so before any privacy-related questions were asked. So we make a tentative conclusion that Android users seem to be more privacy-aware than iOS users, confirming hypothesis H2. We note, however, that this issue needs further investigation. (Reinfelder, Benenson, and Gassmann 2014, 10)

To connect this statement to a cultural comparison is no simple task. It might appear as though German participants in this study, all Android users, are more privacy-aware. However, in regards to culture, I cannot confirm this statement. I can only speculate how German students might behave as Apple iPhone users, but I would hypothesize that their behavior and attitude would be very similar to their American counterparts'. I assume they would not go into their iPhones' setting to verify and/or change the privacy setting after the installation of the Perfect Piano app or any other app.

I certainly think this warrant further research. Findings in this study are contrary to the findings of Joeckel, Dogruel, and Bowman (2017), who proclaim:

> While seven Germans mentioned looking at app permissions for the flashlight, three for the running app and five for the dictionary, none of the US participants mentioned permissions when deciding which app to download for any of the three app searches.

> This lack of attention to privacy permissions among US participants is reflective of other research showing privacy concerns to be rather low among this population. (2017, 630)

The current research study cannot support the claim in this quote.

In this study the American participants, especially those with an Android phone, showed similar privacy concerns, and surprisingly, the only student who refused to download the app due to privacy issues was an American participant. Therefore, I think the result of this research is more similar to what Pentina et al. (2016) affirm:

> Millennial mobile app users in both countries intend to download and continually use mobile apps that require access to personal information in order to satisfy their a) informational and b) social needs … perceived privacy concern does not appear to play a role in the adoption or future use intentions of private-information sensitive apps in either the US or China. This finding, together with the high levels of privacy concern in both countries (US mean. 5.36 and China mean. 5.61 on the scale of 1-7), supports the privacy paradox phenomenon. (2016, 417)

This claim is supported in the current study: in both cultures, there is an attitude behavior discrepancy. Most students illustrate privacy-conscious attitudes during the app-downloading experiment but in the end their behavior does not reflect this as most of them still download and use the app. For me, this shows that the privacy paradox is transferable to smartphones, which I call the mobile privacy paradox.

Concluding I do not perceive mobile privacy attitude and behavior differences between the American and German participants.

9.2.5.4 App Experiment Favorite App Behavior and Attitude

9.2.5.4.1 Similar Aspects between German and American Students

Participants can be divided between those who are pretty well informed and knowledgeable about what types of personal information their favorite app has access to. Furthermore, the students who are somewhat unaware depict mobile privacy complacency behavior and attitude. Here, the three different types of mobile privacy behavior (described in subchapter 9.2.5.1.1) are applicable again: proactive and knowledgeable mobile privacy behavior and attitude (Type 1), moderate knowledgeable proactive mobile privacy behavior and attitude (Type 2), and mobile privacy complacency behavior and attitude (Type 3).

All Americans and nearly all (8 out 10) German students admit to never reading the privacy policy of their favorite app. This attitude and behavior concerning privacy policies for online services and apps are transferrable investigated to what a recent study (Obar and Oeldorf-Hirsch 2018) confirms:

> Individuals often ignore privacy and TOS [Terms of Service] policies for social networking services. This behavior appears to be common both when signing up for new services and when policies change for services individuals are already using. When people do read policies, they often remain on the relevant pages just long enough to scroll to the 'accept' button, and in the few instances where detailed reading takes place, almost all participants demonstrate reading times far below the average reading time needed. (Obar and Oeldorf-Hirsch 2018, 13)

In the subchapter privacy policy, I deliberate on particular participants' privacy policy attitude.

Another finding specific to both cultures is the difficulty in finding the privacy policy of participants' favorite app. As also discussed in the previous chapter, privacy policies are just not easily discoverable in the app stores nor in their favorite some app itself. Interestingly, some participants display mobile privacy complacency behavior and attitude again – they seem somewhat overconfident and therefore, they do not need to know about the privacy policy of their favorite app. And as previously discussed, trust also plays a role in not expressing the need to be familiar with an app's privacy policy.

9.2.5.4.2 Unique Aspects of American Students

Finding the privacy policies for their favorite app proved to be less challenging for the US students; only three of them had issues as opposed to six of the German students.
This might not be related to students' behavior and attitude, but rather I assume it might either depend on the fact that their favorite app includes an actual privacy policy or it may be due to the specific privacy menu[64] included with the Apple iPhone's mobile operating systems settings.

9.2.5.4.3 Cultural Comparative Summary

I observe no behavior and attitude differences when it comes to student's favorite apps.

[64] on the Android mobile operating system, it seems more complicated to control privacy https://www.wired.co.uk/article/android-privacy-settings-oreo-security

9.2.5.5 Privacy Policy Attitude

9.2.5.5.1 Similar Aspects between German and American Students

This study's results corroborate the findings of a multitude of previous work on privacy policies such as McDonald and Cranor (2008); Martin (2013); Park (2013); Ermakova et al. (2014); Slavin et al. (2016); Koohikamali (2016); Aïmeur, Lawani, and Dalkir (2016); Ginosar and Ariel (2017); Story, Zimmeck, and Sadeh (2018); and Brandtzaeg, Pultier, and Moen (2018) inasmuch as all participants think that privacy policies are too long and too complicated to read.

Obar and Oeldorf-Hirsch (2018), confirm this shared sentiment:

> 'Privacy policies are too long', 'There are too many privacy policies to read,' and 'I don't have time to read Terms of Service agreements for every site that I visit.' Privacy and TOS policies were seen as more of a nuisance than anything else (Obar and Oeldorf-Hirsch 2018, 15).

Spensky, et al. (2016) address the difficulty users have in understanding privacy policies, as:

> On both Android and iOS, on average, [they] require a college reading level. That very few of the policies, on either platform, were understandable at a high-school reading level. Thus, while these policies are supposed to serve as the primary tool for conveying privacy-related information to users, they are likely incomprehensible for a large fraction of the population and, for the most part, ineffective (Spensky et al. 2016, 14).

I again associate participants' attitudes with mobile privacy learned helplessness. Students feel that they have no choice or control in the matter and, therefore, will not even try to read the privacy policies since they already expect not to understand them. This also comports with the two students' – one American and one German — distrust of a privacy policy's real purpose: they believe it is the objective of companies and app developers to make them un-user-friendly. Aïmeur, Lawani, and Dalkir affirm the opinion of these two participants since:

> In fact, privacy policies sometimes purposely use incomprehensible vocabulary and the way most of them are written serves to protect the organization from potential privacy lawsuits rather than address user privacy concerns (Earp, Ant_on, Aiman-Smith, & Stufflebeam, 2005). (Aïmeur, Lawani, and Dalkir 2016, 372)

The final corresponding attitude this current study supports is the evidence that several participants from both cultures illustrate something of an arrogant attitude regarding not reading or needing to read a privacy policy.

One possible explanation for German students' level of arrogance reconsiders Hofstede's power dimension since "privacy protection in the U.S.A. – country low on UAI [UNCERTAINTY AVOIDANCE INDEX] – is in most cases left to industry self-regulation, [while] Germany has a large body of laws aiming to protect [the] privacy of its citizens [4]." (Krasnova and Veltri 2010, 3).

For American participants, the assumption is that since most of them are Apple iPhone users, and they believe Apple is a company that supports consumers' privacy, and therefore the students feel their mobile privacy is protected. Another explanation might be again American student's mobile privacy complacency behavior and attitude

9.2.5.5.2 Unique Aspects of American Students

Remarkably, only American students came up with a suggestion on how to improve privacy policies. One reason could be Hofstede's dimension of long-term orientation which is significantly lower than compared to Germany's, since "in short-term-oriented cultures, main work values are freedom, rights, achievement, and thinking for oneself" (Hofstede and Minkov 2010, 497).

Hitherto attempts to tackle the complex issues surrounding privacy policies that have been made by scholars and practitioners. For example, Schaub, Balebako, and Cranor recommend that "privacy notices and controls should become embedded in the user's interaction flow rather than being relegated to lengthy privacy policies and take-it-or leave-it "choices" (2017, 76).

Or as Brandtzaeg, Pultier, and Moen (2018) propose:

> Terms of use and privacy policies [need] to be more reader- and privacy-friendly, but even more important is the need for "privacy by design" and the minimization of data collection by apps. Mobile apps should adopt an industry standard to build trust, making it easier for users to understand where data are traveling and what purpose data are used for. Visualizations, like Figures 4–9, may facilitates understanding and transparency of the dataflow in apps and, as such, make privacy control easier for users. (2018, 484)

And the European Union and Agency for Network and Information Security notes that:

> Privacy policies and notices are more difficult to read on a smartphone and require special attention. As a result, privacy policies should be built using a "layered" approach

> where the most important points are summarized, with more detail easily available if the user wants to see it. Additionally, good graphical design, including use of colours and symbols, can help users understand better [22]. (2017, 12)

And just very recently, Kununka investigated "user centric privacy policy modelling" (2018), which:

> Engages non-technical users in the design of user-centric privacy policy representation. It provides a comprehensive privacy policy information scope that is easily navigable. It facilitates improved understanding of privacy and enhances control over several privacy areas, especially over monetization. It depicts a policy representation that is comprehensive, informative and provides user control over privacy. (2018, 141)

I certainly welcome the American participants' suggestions on how to improve privacy policies. At this point, it seems companies are primarily more concerned with covering the legal aspect and less so with transparency for customers, as "currently, users may not be sufficiently informed at all times about potential personal data collection by app store operators or providers of value-added services they make use of" (European Union and Agency for Network and Information Security 2017, 13).

The chapter on future research recommendations returns to privacy policies.

9.2.5.5.3 Cultural Comparative Summary

I do not observe in the findings any difference between American and German students. The unique findings for the American Students do not affect mobile privacy behavior and attitude.

9.2.5.6 Personal Information and Data – Attitude

9.2.5.6.1 Similar Aspects between German and American Students

Students are quite knowledgeable about the *what*, such as contacts and phone numbers. I assume that when it comes to more in-depth and detailed knowledge and understanding participants from this study mirror what Van Kleek, et al. (2017) point out:

> Faced with this opaque world of data harvesting, smartphone users have been left feeling that they lack adequate understanding to make informed decisions regarding their privacy [17, 21, 34, 48]. As a result, some users have chosen to withdraw from using apps to their full extent, in an attempt to limit data exposure [11, 40, 41]. Previous research has shown that users have skewed expectations about how their data are

> being collected and by whom [26, 29], and overestimate the procedures in place to vet which apps are available through app stores [27] (2017, 5208).

During a field study on mobile app privacy nudging, Almuhimedi, et al. (2015) discovered how people reacted after they had received a more detailed report on what personal information an app shared and how frequently it was shared:

> In the interviews, all eight participants indicated that frequencies of access to personal information by apps were the element of the nudge that caught their attention. For instance, P10 explained: 4182 [times] are you kidding me? It felt like I'm being followed by my own phone. It was scary. That number is too high." P17 stated: "the number was huge [356 times], unexpected. Again, big number a bit unexpected. (2015, 15)

I certainly notice in this current study that participants expressed similar feelings of uneasiness and discomfort once they were shown the ratings for Perfect Piano. The same thing happened once students deliberated the "what" of personal information an app might have access to.

Both cultures also remark on the lack of transparency for smartphone users regarding the *what*, the *with* and the *with whom* when it comes to their personal information since:

> Information about us is collected, stored, analyzed, transmitted and/or sold/purchased by private, for-profit companies without much regulation. Data brokers "are collecting, analyzing and packaging some of our most sensitive personal information and selling it as a commodity... without our direct knowledge" [49]. This multi-billion dollar industry is greatly unregulated due to the lack of public policy in favor of the consumer. (Correia and Compeau 2017, 4021)

Nevertheless, providing people with more knowledge and transparency about what personal information an app can access during the briefing part of the data collection of the interviews shows how a solution for transparency might mean developing a different privacy attitude and behavior in people. This is supported by Brandtzaeg, Pultier, and Moen, who write that:

> Mobile app services should use visualizations to enhance transparency of personal dataflows in mobile apps to make it easier for users to make choices about their privacy. In order to strengthen user trust, it is important to use privacy by design through opt-in data sharing with the service and third parties, and more transparency in personal data sharing practices. (Brandtzaeg, Pultier, and Moen 2018, 485)

When discussing the *with whom*, all students mention the four major tech companies: Google, Facebook, Apple, and Amazon. Zuboff confirms my participants' thoughts about the major

players, with Google being among the first to discover the economic value of personal information (Zuboff 2019, 9, 63–97).

Microsoft is not mentioned at all — which makes sense since Microsoft does not play a significant role in the mobile phone market. From my observations, Google and Facebook seem to be at the forefront of participants' minds when discussing the *with whom*. This is not a surprising finding as these two companies are probably the most prominent tech companies. In addition to these four major tech companies, some students bring up data analysts or brokers, but none of the participants bring up a specific company. Confirming the obtuseness and opacity of all involved stakeholders, Christl and Spiekermann (2016) declare:

> Actually, there are thousands of companies and services, to whom personal data from both website visits and from the use of smartphone apps is transferred. At this point in time, the sector is rather nontransparent and little is known about most of these companies, which might be due to a lack of systematic research as well. (2016, 88)

In the current study, only two students (one from each culture) bring up mobile cell phone provider, which I found unusual. However, upon further investigation, I was unable to find a substantial amount of scholarly research on mobile service providers.

Overall, I recognize three different categories of attitudes in both cultures:

- *Mobile privacy complacency*, has been explored and applied several times throughout the discussion in this chapter.
- *Mobile privacy pragmatism*. I define it as having a realistic attitude toward and the acceptance of the fact that personal information is an afterthought after commodity, with some even calling it the "new oil" (see, for example (Schwab et al. 2011, 5) and (Couldry and Yu 2018, 4476)). An information pragmatist is willing to give away their personal information for a free app or service. Moreover, I posit that a mobile privacy pragmatist is also a realist. They understand that there is no *real choice* in terms of whether or not to give away their personal information.
- *I call it mobile privacy objection.* I define this as a student who has a positive attitude toward sharing and the collection of their personal information and data. This student desires the personalization of their apps and services. Furthermore, they are also in favor of having their data used to improve services and apps.

9.2.5.6.2 Unique Aspects of German Students

More German students brought up the NSA, secret services, or other governmental entities in conjunction with the sharing of their personal information.

- First, I speculate that this is primarily due to Germany's fraught history with privacy and surveillance.
- Second, the NSA surveillance revelation by Edward Snowden (see, for example, Landau 2013) sparked a significant outcry within German society. It brought the debate on government, surveillance, and privacy to the forefront with the "denial of knowledge to denial of participation, acknowledgment of limited participation and, finally, to complaining about the monitoring of Angela Merkel's[65] cellphone" (Schulze 2015, 197). I could see this as the primary reason the German participants were more likely to associate NSA et al. to the topic of personal information sharing.
- The third motive might have to do with Hofstede's cultural dimension (see chapter 3.4.1). Germany rates high on the Uncertainty Avoidance Index (UAI) and, as such, laws and regulations are highly established. Krasnova and Veltri confirm this by stating, "high level of UAI in society typically leads to stricter laws which protect individuals. Empirical evidence shows that these laws may work to reduce the privacy concerns of consumers [14] " (2010, 5). It might be due to the fact that German students believe their personal information should be protected by law against the intrusion of governmental and secret services.

9.2.5.6.3 Cultural Comparative Summary

Besides the unique feature for German students above, I do not perceive a major cultural disparity in US and German students' feelings and opinions. All students seem to know the what, the why, and the whom concerning their personal information and data being shared. Moreover, I discover within all twenty participants across both cultures' mobile privacy complacency and mobile privacy pragmatism.

[65] Chancellor of Germany 2005 until today (February 2020).

9.2.5.7 Transparent Human *(Der gläserne Mensch)* – Attitude

9.2.5.7.1 Similar Aspects between German and American Students

One thing all participants have in common: they do not want to become a "completely transparent human (*gläserner Mensch*). Participants do not want to allow companies, governments, or both to track, collect and disseminate their personal information. Comparing this attitude with at the beginning of this chapter discussed themes privacy and mobile privacy, I see some parallels among students' attitudes about being or becoming transparent. Students *do* want to keep certain parts of their lives private and would like to have control over what they either self-release about their lives or what others might be able to collect and share about them.

This attitude, shared by both cultures, is supported by two recent studies – one focused on each culture. In the United States, in 2019:

> Fully 79% of adults say they are at least somewhat concerned about how companies are using the data it collects about them, including 36% who say they are very concerned about this issue. At the same time, 64% of Americans report they feel very or somewhat concerned about how the government is using the data it collects about them. (Auxier et al. 2019)

Furthermore, in a study conducted in Germany in 2018:

> It turned out that the Germans are fundamentally concerned about their privacy. This results in a slightly higher value for online contexts (e.g., surveillance by the NSA) in contrast to offline contexts (e.g., camera surveillance in public places) … For Germans, privacy is sacred!
>
> *(es zeigte sich, dass die Deutschen grundsätzlich besorgt um ihre Privatheit sind. Dabei ergibt sich ein leicht höherer Wert für Online-Kontexte (bspw. Überwachung durch die NSA) im Gegensatz zu Offline-Kontexten (bspw. Kameraüberwachung auf öffentlichen Plätzen)...'Den Deutschen ist ihre Privatheit heilig!')* (Braun and Trepte 2018, 6,9)

To me, this also emphasizes how both cultures value and respect privacy and its subset mobile privacy as a fundamental construction that has to be conserved within an ever-changing global digital society. This somewhat surprising core belief regarding privacy and mobile privacy is a finding that I did not expect to discover — at least as a theoretical or abstract point of view for the American students. Even though I would cautiously argue (see below unique US aspects) that the Americans exhibit a more rational and at times soberer attitude about

the real possibility to have, keep, and maintain mobile privacy. Overall, both nationalities reject total personal information transparency.

In his essay "'*I've Got Nothing to Hide' and Other Misunderstandings of Privacy*," Solove (2007) counterargues the call for data transparency by declaring:

> Most replies to the nothing to hide argument quickly respond with a witty retort. Indeed, on the surface it seems easy to dismiss the nothing to hide argument. Everybody probably has something to hide from somebody. As the author Aleksandr Solzhenitsyn declared, "Everyone is guilty of something or has something to conceal." … As one comment to my blog post noted: 'If you have nothing to hide, then that quite literally means you are willing to let, me photograph you naked? And I get full rights to that photograph—so I can show it to your neighbors?'. (Solove 2007, 750)

Interestingly, there were other subthemes that emerged from both cultures in my study group— such as the tech companies (Google, Facebook) and their dominance, as well as law and regulation, and awareness and education.

When it comes to law and regulation, I find it surprising how many (see below American students for further discussion) American participants present this as a possible solution. Which reveals another similarity both cultures bring about possible solutions that would resolve the conundrum of how to be a global, digital citizen who also values control over his or her personal data. This exemplifies to me even further that younger adults want privacy and its subset, mobile privacy.

Nevertheless, students did display both mobile privacy pragmatism and mobile privacy complacency attitude and possible behavior again. When it comes to behavior I can only speculate, since the actual behavior observation in this study was for a given task. Another possible reason for both of these traits are two theories that have been widely discussed in the literature: the privacy paradox and the privacy calculus theory.

The privacy paradox is, in my opinion, transferable to smartphone behavior and attitude. Thus, I call it the mobile privacy paradox. Yes, in theory, neither cultural group wants to become transparent humans, but their actual behavior often differs quite dramatically from this. As I state before (see mobile privacy learned helplessness) while I clearly see evidence of a mobile privacy paradox I prefer as a possible explanation for this phenomenon what I call

mobile privacy learned helplessness. Yet I also need to point out that at this stage of this research it might be too early to have enough proof.

When it comes to the privacy calculus theory (see chapter 3 Pentina et al.), which weighs perceived benefits against perceived risk before the possible disclosure of personal information, I also see the privacy paradox as it exists in both cultures. Moreover, it might also be transferrable to the smartphone world — what I call a *mobile* privacy calculus theory.

The last subtheme, awareness and education, will be discussed in detail in chapter 10. Here I just want to highlight how American students perceive education:

> Students in our study expressed helplessness in the face of powerful corporations, they became motivated to challenge them as they learned more. This faultline between the perception of helplessness and a desire to create change is a productive site of emotional friction that opens opportunities to engage in "education for democracy."… This education for democracy — both formal and beyond — can empower us to reclaim our role in shaping the future. (Head, Fister, and MacMillan 2020, 34)

9.2.5.7.2 Unique Aspects of German Students

From my perception, German students have a more stringent attitude toward, and less complacency about, not being or becoming a fully transparent human *(ein gläserner Mensch)*. From my point of view, many possible explanations are related to culture.

- One possible reason could be Germany's troubled history with privacy (see also literature chapter 3). Therefore, students might exhibit greater fears about losing their privacy to the State again.
- Another reason for German students' anti-transparent human stance is again connected to Hofstede's cultural dimension. Here, I see two possibilities that fit:
  - The first is the dimension of the individualism, which is, according to Reay, et al., (2018) "unsurprising. Highly individualistic countries can intuitively be expected to embrace the idea of an individual's 'private space' as a social norm; prior research (Hofstede 1980, 1991; Milberg et al. 1995) supports this idea" (Reay, et al. 2018, 282). Comparing this with a recent survey by Braun and Trepte (see also above related aspects citations) Germans perceive data privacy as the *most crucial* privacy

categories they want to be able to control – as compared to, for example, physical or social privacy (2018, 7).

- The second correlated dimension is the Uncertainty Avoidance Index (UAI), with Germany's score of 65% as compared to 45% of the United States ("Country Comparison" 2019). And "societies with a high Uncertainty Avoidance Index (UAI) tend to reduce uncertainty by embracing clear written rules and regulations, and maybe more likely to introduce higher levels of government regulation of privacy." (Bellman et al. 2004, 3). I hypothesize that this study's German participants believe that these laws will protect their personal information in a global digital world. Therefore, it seems like a likely perception of German students that laws will prevent individuals from being or becoming a completely transparent human.

Unfortunately, recent research from 2018 — conducted with Norwegian population and mix of Norwegian as well as U.S.-based apps — contradicts the notion that strict laws always have an impact of personal information sharing:

> This study found that most data, including personal data, are transferred from Europe to the United States, even from native Norwegian apps, which prove how personal data are traveling across the Atlantic Ocean. This might be a problem as the United States and Europe exhibit different approaches to information privacy; Europe has stricter privacy laws than the United States (Smith, 2001). For European app users, and in this case Norwegian app users, this also means that big American tech companies seem to process personal data for multiple purposes. (Brandtzaeg, Pultier, and Moen 2018, 483)

9.2.5.7.3 Unique Aspects of American Students

In terms of defining an attitude, there are three things that strike me as specific to American students:

- I more often recognize in the American students what in this study I define as mobile privacy complacency as well as mobile privacy pragmatism. This notion is supported by the authors of the study "Information literacy in the age of algorithms" (2020):

  > An important takeaway from our focus groups was the profound ambivalence — the tangle of resignation and indignation — that almost all students expressed about algorithm-driven platforms that collect data about their personal lives. While many students objected to certain advertising practices platforms used, they were nonetheless resigned to using sites like Google and YouTube. In their words,

algorithms were "part of the deal" if they wanted to use free apps (Head, Fister, and MacMillan 2020, 14).

This may also show that while the mobile privacy paradox exists for American students, too, it might be less pronounced. However, I cannot speculate about this since this study offers limited data regarding behavior.

- Furthermore, a somewhat surprising finding is that more American students talk about laws and regulations as a countermeasure to being or becoming a transparent human *(Gläserner Mensch)*. At first, I was taken off guard by this finding, given that, historically, the U.S. and U.S.-Americans seem to have been in favor of deregulation when it comes to privacy. Moreover, given that almost all innovative digital technical inventions have come from the United States (Apple iPhone, apps, social networking sites, etc.) it seemed that most of the German and American students in this study would repeat what Downes (2018) suggested as a solution: "to stay the course, to continue leaving tech largely to its own correctives — is cold comfort to those who believe tomorrow's problems, coming up fast in the rear-view mirror, are both unprecedented and catastrophic" (2018, para. 25). However, Downes wrote this article one month before the Facebook Cambridge Analytica scandal broke (early 2018). I would argue that this scandal has had a positive impact on American's perception of how to better regulate data and mobile privacy. In the discussion of Fieldwork 2, I will further examine American attitudes on privacy laws.
- Moreover, the American students addressed to a much greater degree ethics, morals, and the philosophical side companies should adopt when it comes to personal information transparency (the German students did discuss societal development). This is quite contrary to my initial observation (see chapter 1 Personal Background) that American students do favor personal information and transparency over privacy laws. At this point I do not have an explanation why more Americans talk about ethics, morals, and responsibilities tech companies might have to society at larger. It certainly would be worthwhile investigating further.

9.2.5.7.4 Cultural Comparative Summary

I do seem to discern a stronger attitude from the German students in regard to being a transparent human. The Americans show more realism, or what I call mobile privacy pragmatism. However, it's not easy to come to an unambiguous result. I somewhat cautiously declare that the difference in the attitudes are outweighed by the similarities in their actual behavior similarities.

9.3 WhatsApp Behavior and Attitude – German Students

I was unable to compare the messenger app WhatsApp between the two cultures, due to its relatively low market share in the U.S.:

> WhatsApp has a market share of 95% in Germany, whereas in the US the market share is 34%. Facebook Messenger has a 49% market share as compared to 86% in the U.S. Telegram and Signal have 8% and 2% in Germany, and in the U.S., it is 7% and 2%. Threema is not listed in the US, but it has a 3% market share in Germany. *("Which Messenger Services Do You Use Regularly?" Chart. April 23, 2019. Statista. Accessed August 15, 2019*)[66]

Some German students seem more likely to display what I call proactive and knowledgeable mobile privacy behavior and attitude. Ergo, they are using alternative messenger apps. This finding for Germans is supported by De Luca, et al. (2016) by stating as one reason for using a particular messenger that "privacy and security, only a small fraction of participants stated this being their main factor. An exception is Germany, in which it is the third-most important factor with 13.12%." (2016, 149).

All German students are aware that WhatsApp belongs to Facebook, and by actively choosing an alternative to WhatsApp, they are taking a stance against a big global corporation. I would call this somewhat an active act in the attitude as well as behavior in that they are not giving all of their mobile data and personal information to a monopoly (Facebook, Google, Amazon). Yet, even though German students seem to be more concerned about mobile privacy when it comes text messaging services, I discern in the findings that this behavior and attitude is more due to Facebook antipathy than due to mobile privacy concerns.

[66] Interestingly the statistics does not include any market share for iMessage, Apple's messenger app; no other source was found for iMessage market share.

Yet my findings support the claim that "despite security and privacy playing a role in the decision making process for some people, they were only seldom the primary factor, while peer influence, i.e., who and how many people use the IM, was identified as the most important factor." (De Luca et al. 2016, 156).

9.4 Mobile Security Behavior and Attitude

9.4.1 Similar Aspects between German and American Students

As the data suggests, German and American students bring up mobile security features without being explicitly asked about it. These findings document that all research participants are aware of, and use to some extent mobile security options and features.

But I observed and agree with Li and Clark (2013) claims, since "one central problem, however, is the inability of users to make good security choices. As studies show, typical users have neither the necessary understanding of the available security mechanisms nor the ability to properly utilize those protection mechanisms to their full benefit." (2013, 78).

Another unusual behavior I observe in several participants from both cultures is contradictory and inconsistent behavior when it comes to mobile security. For the U.S. participants, this behavior is linkable to a Pew Research Center survey (2017), which states:

> That Americans are not always vigilant in the context of mobile security. For instance, 28% of smartphone owners report that they do not use a screen lock or other security features to access their phone, while around one-in-ten report that they never install updates to their smartphone's apps or operating system. Meanwhile, 54% of online adults report that they utilize potentially insecure public Wi-Fi networks – with around one-in-five of these users saying that they use these networks to perform sensitive activities such as e-commerce or online banking (Olmstead and Smith 2017, 5).

To my knowledge, no similar survey data is available for Germans' mobile security behavior. From my observations, I would argue that the German participants' response would be similar to the Pew Research survey results.

A last unexpected finding was the confusion of mobile privacy with mobile security, which is a phenomenon I also discuss as well as in Fieldwork 2. While the distinction was always logical, this mix-up occurred not only with my research participants, but I observe it while talking about my research to friends, relatives, or acquaintances. Many times, a response is along the

lines of "Oh, you are researching security issues on the phone." Therefore, I addressed the distinction between those two topics in chapter 2, as well as chapter 3. Indeed, this confusion is not a new phenomenon. As early as 2006, Zheng and Ni acknowledge that "security issues in mobile computing environment are closely related to privacy issues" (2006a, 392), and emphasize that "mobile privacy is more complicated than mobile security because you cannot just draw a line between what information can be used or shared and what cannot, whereas in security we know that a set of security functions should be implemented in a system" (2006a, 393). A more current article on the complexity of these two topics supports my findings, as the authors "asked interviewees to define privacy and security, specifically about IoT devices. Their definitions demonstrated that they had a narrow and limited knowledge of privacy and security, and some could not distinguish between them"(Emami-Naeini et al. 2019, 6). A quantitative study points out that "users tend to have increased confidence in the daily use of their mobile devices, leading them to negligent behavior towards actions with potential security-related impact"(Gkioulos et al. 2017, 11).

9.5 Linguistic Highlights

9.5.1 Similar Aspects between German and American Students

It has been my objective to narrate a thick description about participants' attitudes and behavior concerning mobile privacy. As I had indicated in the Research Method chapter language, the words, expressions used by participants might give some further clues concerning attitude and mobile privacy. It is quite interesting for me to observe in participants from both cultures equally potent usage of vocabulary concerning mobile privacy. To me, many of these linguistic terms can be correlated to what I call in mobile privacy complacency. In several instances, these terms imply complacency's heightened form – what I call mobile privacy learned helplessness.

In addition, all participants also exhibit laughter, often nervous laughter or chuckling which I interpret as an expression of discomfort. The laughter also exemplifies mobile complacency and mobile learned helplessness. The findings imply that in both fieldworks, students are fully aware that they do not have a choice, and would like more transparency and control. Thus,

minimizing the situation, I would speculate laughing, or chuckling might alleviate the feeling of helplessness and lack of choice.

As I have pointed out in the scholarly literature chapter 3, there is not much qualitative research currently available. It is therefore not easy for me to correlate the linguistic findings to other scholars. Nonetheless I would like to point to articles that address the linguistic feelings about privacy and mobile privacy.

The first, by Shklovski et al. (2014), has several claims from that are transferrable to my study. For example, encountering as a smartphone user a mobile privacy violation:

> Can result in a range of emotional responses, though it may not necessarily lead to outward action to alleviate the problem. One can be outraged, exasperated, horrified, even cynically bemused. Along with or in addition to these, people often describe their discomfort by referencing the word "creepy." (2014, 2349)

Furthermore, the article's linguistic findings are very relatable to the findings of this study, as they also highlight mobile privacy learned helplessness and mobile privacy complacency. I consider the following responses on smartphone tracking and data collecting prime examples of the two:

> "I silently accept it. When you make me think about it, I kind of don't like it, but have probably forgotten all about it next time I download an app." – survey, Denmark. "It seems like a necessary evil at this point. Because it is so ubiquitous, I think that it's likely that this sort of thing will never go away." – survey, USA. In both cases there is an implicit agreement that the respondent has no way of affecting the situation and must accept it if they are to be able to go on (Shklovski et al. 2014, 2354).

As a solution to this conundrum, the authors call for a "practical theory of creepiness, its varieties, and its temporalities (e.g., does creepiness fade over time with familiarity, and if so, what replaces it?)" (Shklovski et al. 2014, 2355), and point to the need for more future research to examine and possibly define it. This is precisely what Tene and Polonetsky (2013) have done from a social and legal viewpoint. Talking about creepiness, the authors write that "as new technologies strain our social norms, a shared understanding of that alignment is even more difficult to capture. The word 'creepy' has become something of a term of art in privacy policy to denote situations where the two do not line up"(2013, 60). However, the particular relevance of their article for my research is not only the included linguistic expressions but also their suggestions on how to resolve or at least alleviate the privacy conundrum: "As technological innovation accelerates, so does the need to recalibrate

individual expectations, social norms, and, ultimately, laws and regulations." However, they also caution that in "an environment of rapidly shifting social norms and expectations, the law can be a crude and belated tool" (Tene and Polonetsky 2013, 102).

I certainly see this statement fitting into the findings of Fieldwork 2 and the GDPR subchapter.

To solve this predicament, the authors also call for greater collaboration from companies, engineers and all the other many stakeholders involved:

> As with all matters creepy, shining the light is the ultimate strategy, providing individuals with access to their information and insight into the data practices deployed. Finally, individuals should be educated to treat their own data and that of their peers with respect, realizing that in a digital environment prior prudence and restraint are far more effective than any *ex post* clean up effort (Tene and Polonetsky 2013, 102).

9.5.2 Cultural Comparative Summary

I do not find any cultural differences regarding linguistic highlights.

9.6 Summary

In this chapter, the described themes from the findings Fieldwork 1 have been discussed and compared to American and German participants. The following chapter will discuss findings Fieldwork 2.

10. Discussion Fieldwork 2

10.1 Overview

In the following, the findings for Fieldwork 2 are discussed by the following themes: attitude and behavior concerning the Facebook Scandal and GDPR; privacy protection and privacy education. In the last two subchapters, I deliberate mobile security and linguistic highlights.

10.2 Discussion by Theme

10.2.1 Facebook Mobile Privacy Attitude and Behavior

10.2.1.1 Similar Aspects between German and American Students

Overall, I perceive many similar aspects between both cultures:

- All students were somewhat not surprised, and I would even say some somewhat expected a Facebook data breach scandal. I correlate this attitude to what I call in this study mobile privacy learned helplessness. I perceive in all students somewhat a resignation when it comes to protecting their personal information. It does not matter to change behavior since helplessness attitude renders any behavior irrelevant.
- All of the students still use Facebook out of convenience, and because of Facebook's monopoly and worldwide leadership position in the social network market.

  Madrigal (2018) confirms this by declaring:

  > Despite personal reservations about Facebook's interwoven privacy, data, and advertising practices, the vast majority of people find that they can't (and don't want to) quit. Facebook has rewired people's lives, routing them through its servers, and to disentangle would require major sacrifice...Even if one were to quit the core service, there are many other ways of being roped into the Facebook ecosystem. There's Instagram and WhatsApp, sure, but the company also maintains "shadow profiles" on refuseniks. (2018, para. 6,7).

  And:

  > There is no denying that Facebook has a de facto monopoly in the social network market. Around two-thirds of Americans use Facebook, three-quarters of them on a daily basis. In the United States, 80% of user time spent across social networks is spent on Facebook. Through having purchased Instagram and WhatsApp, Facebook now owns the top three, and four of the top eight, social media apps. Like Google, Facebook monetizes its service by selling placement to digital advertisers. There are at least two sets of market participants that both rely on Facebook's network and find themselves

> in competition with Facebook: app developers and online publishers. In both markets, Facebook has used its dominant position to appropriate from. (Khan 2019, 1001)

I perceive that Facebook's omnipresence, combined with its usability and conveniences, all help overcome any privacy concerns.

- Only one student supposedly went through the effort to check her privacy and security settings after the scandal. All the other students considered there setting as secure and private even before the scandal, thus displaying somewhat I cautiously declare as a level of arrogance and overconfidence in their ability to be privacy literate. These behaviors and attitudes are not new as a study from 2015 argues:

  > On sites like Facebook, and it is not obviously the fault of users: successful navigation of the site's constantly changing privacy policies requires a commitment to continually mastering and remastering byzantine detail and complexity. The only seemingly consistent rule is that the software will default to openness. Empirical research repeatedly demonstrates that Facebook users do not successfully effectuate their privacy preferences and that they often do not even know this. For example one recent study found that a full third of Facebook users left privacy settings at their open-sharing default and that nearly two-thirds have actual privacy settings that do not match what they think those settings are—almost invariably in the direction of more disclosure (Liu et al. 2011). (Hull 2015, 93)

- Fieldwork 2 participants' behavior and attitude fit with what I call mobile privacy complacency. Fascinatingly this finding and the one from above (remaining a Facebook user) contradicts results from a study by the Pew Research Center:

  > Most notably, 44% of younger users (those ages 18 to 29) say they have deleted the Facebook app from their phone in the past year, nearly four times the share of users ages 65 and older (12%) who have done so. Similarly, older users are much less likely to say they have adjusted their Facebook privacy settings in the past 12 months: Only a third of Facebook users 65 and older have done this, compared with 64% of younger users (Perin 2018, para. 7)

  However, a Mozilla survey is more transferable, with "few people (24%) reported making changes to their Facebook accounts following the recent news of privacy concerns around Facebook" (Mozilla, 2018, para. 6).

- In both study groups, I observe attitude and desire to be more privacy-conscious, but both study groups do not follow up with actual action and behavior changes. This behavior attests to what I call the mobile privacy paradox.

10.2.1.2 Unique Aspects of German Students

The willingness to pay an annual subscription fee for Facebook, and then in return to have a guaranteed secure and privacy maintaining and respecting social media network was suggested by one German student.

Nonetheless, this is in contrast to the majority of US Facebook users, according to a survey conducted by Mozilla in 2018: "very few people (only 12%) said they would consider paying for Facebook, even a version of Facebook that doesn't make money by collecting and selling personal data." (Mozilla, 2018, para. 4)

I was unable to find current data for Germany. An online survey from 2012 conducted among 1,045 participants from a German and Austrian university (Bauer, Korunovska, and Spiekermann 2012) asserted: "A key result of our study is that almost half of the participants do not value their personal information at all. Across groups, 48.1 percent of the participants state a WTP [Willingness To Pay] of 0 EUR for their data" (2012, 8). I can only speculate whether the percentage would be equally high if the survey were to be conducted now. Though, I would like to point back what one of the German participants said about the paid-for messenger app Threema (see Findings Fieldwork 1). He said that he had to pay for his friends Threema app since none of them was willing to spend the 3 euros for a messenger app that is deemed as protecting user's personal information. Hence, I somewhat cautiously believe that most German Facebook users would also not be willing to pay a fee for a privacy-protective Facebook. Also associating this with mobile privacy complacency and mobile privacy learned helplessness, many German young adults would probably not deem it worthwhile to pay a fee to keep their personal information safe and private.

Another unique finding from the German participants was the self-disclose or self-proclaimed notion of being a conscious app installer. Both students assert to either limiting the number of apps they install on their smartphones. Alternatively, deliberating the pro-and cons before installing an app. This behavior is what I describe and discuss previously as mobile privacy calculus theory. Even though this is an exciting finding, I do not have proof of how students behave in their daily life as conscious app installers. One student admits that her perceived

benefits usually outweigh her perceived risk, and hence she is a prime example of the mobile privacy paradox.

10.2.1.3 Cultural Comparative Summary

Summing up, the Facebook scandal does not seem to have had any impact on students' mobile privacy behavior and attitude concerning the social networking site. I link this to results from the Mozilla survey: "Most people say they are very concerned about the safety of their personal information online. However, most people didn't make any changes to their Facebook accounts following the recent news of privacy concerns around Facebook." (*The Results Are In ...* 2018). The survey results also fit into what Choi, Park, and Jung (2018) declare:

> Although repeated data breaches may increase privacy concern, the public is inclined to underestimate or ignore the risk (Ponemon, 2014). Frequent data breaches may make people feel as though they have no control over personal information, and ultimately drive them into a state of resignation about online privacy (Kwon & Johnson, 2015). (2018, 42)

What I find interesting is how the Facebook scandal seems to have propelled a public discussion on personal information, mobile privacy, and law, especially in the United States. Additionally, it is interesting to observe how Facebook sees or rebrands itself since the scandal as an avid proponent of data privacy regulations (see for example, Zuckerberg 2019a; Zuckerberg 2019b).

. Mark Zuckerberg, CEO of Facebook, said that:

> I believe a privacy-focused communications platform will become even more important than today's open platforms. Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks … I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure, and their messages and content won't stick around forever. This is the future I hope we will help bring about. (Zuckerberg 2019a, para. 2,7)

How serious Facebook is about this paradigm shift can be more easily gauged after the release of a new transparency tool[67] that is:

[67] On January 28, 2020, which is also International Data Privacy Day.

> Giving us a new way to glimpse just how much it knows about us: On Tuesday, the social network made a long-delayed "Off-Facebook Activity" tracker available to its 2 billion members. It shows Facebook and sister apps Instagram and Messenger don't need a microphone to target you with those eerily specific ads and posts — they're all up in your business countless other ways. (Fowler 2020b, para. 5)

Facebook also release a new privacy checkup tool that will:

> Show nearly 2 billion people around the world a prompt encouraging them to review their privacy settings. The prompt will show up in your News Feed and direct you to the Privacy Checkup tool, which we recently updated. This makes it even easier to adjust who can see your posts and profile information, strengthen your account security by turning on login alerts, and review the information you share with apps you've logged in to with Facebook. (Zuckerberg 2020, para. 4)

10.2.2 GDPR Privacy Behavior and Attitude

10.2.2.1 Similar Aspects between German and American

Nearly all participants are aware of the new data privacy law, which aligns with an infographic released by the European Commission:

> 67% of Europeans have heard of the GDPR, and 57% of Europeans know that there is a public authority in their country responsible for protecting their rights about personal data."("Infographic-Gdpr_in_numbers_1. Pdf" n.d.) Furthermore, The EU reports that GDPR has increased European citizens' awareness of their rights. Since taking effect, European DPAs have received almost 145,000 GDPR complaints and have initiated a range of enforcement actions, including issuing fines. (Fefer and Archick 2019, 2)

All students are also in favor of this new law. Even the one American student who did not have previous knowledge about the data privacy law turned out to view it favorably.

Students' attitudes and behaviors in regards to privacy policy does not differ at all from what I discuss in Fieldwork 1. One difference is though that, surprisingly, two students, one from each country, claimed to have read and reviewed updated privacy policies carefully. Each student fits into Type 1 (out of 3) from Fieldwork 1, as they are depicting proactive and knowledgeable mobile privacy behavior and attitude.

10.2.2.2 Unique Aspects of German Students

I tentatively discover in the German mobile privacy learned helplessness. Participants might have been inundated with so many updated and revised privacy policies that they might have

probably just clicked yes without feeling they have any control or choice of the matter. In the scholarly literature, this behavior has also been called "consent fatigue, reflecting the tendency of people to simply accept a privacy policy without reading it (Schermer et al., 2014)" (Choi, Park, and Jung 2018, 43).

It also seems to detect in German students somewhat an attitude of superiority and maybe even a bit of arrogance when it comes to the implantation of the new law. This might be linkable to Hofstede's dimension of Uncertainty Avoidance Index (UAI) again, since Germany has a high level of UAI as compared to the US. Thus, strong data privacy laws have been in existence for quite some time. However, I also cautiously argue that this might make the German participants a bit more careless in their mobile privacy attitude in regards to foreign-based apps. Since they might think they are protected and thus do not need to be too privacy-conscious. Furthermore, there's a difference between knowing that a law exists and knowing what that law means in terms of individual data protection. Trepte and Masur confirm this:

> Germans' online privacy literacy is moderate. Although many citizens are quite aware of data collection and analyses by online website providers, they are not very knowledgeable about their rights and data protection laws. They generally know about technical aspects of data protection, but it is specifically older people who lack sophisticated data protection strategies. (2017, 6)

10.2.2.3 Unique Aspect of American Students

Similar to findings and discussion Fieldwork 1, only American students bring up suggestions on how to improve privacy policies. Besides the explanation in discussion 1 (see chapter Privacy Policy Attitude), it also is worth looking at Hofstede's Individualism dimension, which is relatively high for the US, with 91% versus Germany's 67%. Hofstede claims that in the USA, "in the business world, employees are expected to be self-reliant and display initiative" (*Country Comparison Germany and USA* 2019, para. 6). It might be possible then then that in the US students are also more trained and educated on finding practical solutions for a problem.

10.2.2.4 Cultural Comparative Summary

A comparison of the discussed aspect above does not reveal cultural disparity as having an impact on the student's overall mobile privacy attitude and behavior.

10.2.3 Privacy Protection Attitude

10.2.3.1 Similar Aspects between German and American Students

Three students, Jan, Beate and Meghan, think that privacy protection should be regulated, primarily via governmental laws.

For the German students this finding is not surprising since I trace it back to Germany's data privacy history as well as Hofstede's dimension of UIA, which shows that "countries with high scores on uncertainty avoidance tend to be characterized by high levels of rules and structure (Triandis, 2004), as they place high value on law and regulations in organizations, institutions and relationships (Hofstede, 2001)" (Giebels et al. 2017, 94).

Interestingly one of the American students changed his mind during the interview. At first, Zachary was not in favor of the American government in charge of a data privacy law, which is contrary to what he stated earlier during our GDPR discussion. Zachary's skepticism about the US government's ability to protect his privacy corresponds with a study by the Pew Research Center: "Roughly half of Americans do not trust the federal government or social media sites to protect their data" (Olmstead and Smith 2017). Zachary's hesitance about governmental involvement can be linked again to Hofstede's cultural dimensions, since "the fairly low score on Power Distance (40) in combination with one of the most Individualist (91) cultures in the world reflects itself in the following: The American premise of 'liberty and justice for all.' This is evidenced by an explicit emphasis on equal rights in all aspects of American society and government" ("Country Comparison Germany and USA" 2019, para. 6). Moreover:

> America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home. The prime danger, from the American point of view, is that "the sanctity of [our] home[s]," in the words of a leading nineteenth-century Supreme Court opinion on privacy, will be breached by government actors. (Whitman 2003, 1161–62).

Nonetheless, in these findings, I observe a shift in the attitude of the US participants in favor of more federal regulation to protect their personal information. This is linkable to what a Pew Study from 2019 found out:

> When asked how much government regulation there should be around what companies can do with their customers' personal information, 75% of adults say there should be more regulation than there is now. About one-in-ten (8%) feel companies should be regulated less than they are now, while 16% say there should be about the same amount of regulation. (Auxier et al. 2019, 43)

Moreover, since the Facebook scandal and the implementation of the GDPR there have been more discussions in the mainstream media.[68] And the scholarly literature (see, for example (Boshell 2018) and (Meyer 2018)) and US government (see (Fefer 2019)) about a possible federal data privacy law.

Two students – one from each culture, Zachary, and Beate also express their distrust about companies to safeguard their personal information and data. Interestingly, these are the same students who somewhat distrust the government in protecting their personal information and data. Trust and distrust seem to be closely connected to consumers' attitude on personal information tracking, collection, and dissemination:

> A firm that is considered untrustworthy will find it difficult or impossible to collect certain types of data, regardless of the value offered in exchange. Highly trusted firms, on the other hand, may be able to collect it simply by asking, because customers are satisfied with past benefits received and confident the company will guard their data. In practical terms, this means that if two firms offer the same value in exchange for certain data, the firm with the higher trust will find customers more willing to share. For example, if Amazon and Facebook both wanted to launch a mobile wallet service, Amazon, which received good ratings in our survey, would meet with more customer acceptance than Facebook, which had low ratings. In this equation, trust could be an important competitive differentiator for Amazon. (Morey, Forbath, and Schoop 2015, 79–80)

And as Tene and Polonetsky (2013) point out:

> Users may trust recognized brands more than they do newcomers, but this approach does not imply that recognized brands have a de facto license to use data in a manner that start-up businesses do not. Rather, the point is that user perception of a brand can

[68] Such as https://www.consumerreports.org/privacy/consumer-online-privacy-rights-act-could-safeguard-data-but-tough-fight-lies-ahead/, https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html, and https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html

> help a company that is proposing new data uses if such uses constitute an extension of the brand that resonates with consumers. For example, a consumer does not ordinarily expect his sneakers to communicate with his phone, but if Nike sold a Nike brand smartphone, consumers would be more likely to expect it to communicate seamlessly with their bluetooth-enabled Nike shoes. (Tene and Polonetsky 2013, 91)

This distrust in companies that both students express exemplifies what I call in this research mobile privacy learned helplessness.

As a last similarity to discuss is one attitude all students have in common. All participants think that the protection of personal information is also their responsibility. This seems to be not only the opinion of the interviewees but also currently I would assume the status quo:

> Looking at the status of individuals as data subjects in current approaches toward privacy and data protection, one can detect a great weight being placed on individual agency and personal responsibility in managing risks of data exposure. Particularly in the United States, self-management and informed user consent have been guiding principles in people's interactions with data collecting organizations (Solove, 2013). Informed consent puts the burden on the individual to control which personal data he or she discloses and under which conditions. (König 2017, 7)

While I, to some degree, agree with participants' opinions, I also perceive it somewhat as an imbalanced solution and even somewhat a burden to put the responsibility first and foremost on the individual. Which is what Crabtree et al. already assert:

> The view offered here is that new data protection regulations being put forward in the USA and adopted in Europe are also about enabling a new kind of economic actor: an actor who is an active player in, rather than a passive victim of, the digital economy in general and the emerging data economy in particular. From this point of view, proposed data protection regulations can be seen to promote the data economy by creating legal frameworks that shift the locus of agency and control in data processing towards the individual consumer or 'data subject.' (2016, 947)

However, as this research has shown, leaving the responsibility on the data subject seems a too-easy solution. The findings and the discussion have repeatedly shown that the average smartphone user response is helplessness, complacency, or pragmatism. Boerman, Kruikemeier, and Zuiderveen Borgesius (2018) delineate that:

> Self-management of online privacy seems particularly important as the law only provides limited privacy protection. First, in many countries, the law is not fully prepared for modern data processing practices. Even if lawmakers and regulators want to protect privacy, they are struggling with the question of how to provide effective legal privacy protection. Moreover, even if up-to-date privacy laws are in

> place, enforcement is often insufficient. Regulators have limited resources to make companies comply with the law (Boerman, Kruikemeier, and Zuiderveen Borgesius 2018, 2).

Additionally, Trepte and Masur (2017):

> Research has shown that Internet user are often not able to adequately protect their privacy. In recent debates about data protection and online privacy, privacy advocates and scholars alike have stressed the importance of online privacy literacy as a "principle to support, encourage, and empower users to undertake informed control of their digital identities" (Park, 2013, p. 217). It has consequently been said to be a precondition for informational self-determination. (2017, 43)

10.2.3.2 Cultural Comparative Summary

From my viewpoint, I only discover similarities and no differences in students' attitude for the theme of privacy protection.

10.2.4 Privacy Education Attitude

10.2.4.1 Similar Aspects between German and American Students Attitude

All participants share the same attitude when it comes to privacy education: it should be included in the educational curriculum from a very early age. Moreover, they all agree that privacy education should be part of broader subjects such as informatics or information literacy. This suggestion is supported by Cohen (2018) who states:

> By the time children start school, most have already figured out how to turn on the tablet, find apps on Dad's smartphone, and search the favorites tab for their preferred websites. But they still have a lot to learn about staying safe online … this is why it's important that students become savvy digital citizens who are able to both enjoy the benefits of being online and avoid potential pitfalls. Young people need to be equipped with the knowledge necessary to navigate the online world and participate in the digital domain in a privacy protective manner. (Cohen 2018, para. 4,6)

Other scholars have supported the need for privacy education and awareness; see, for example, Park (2013) and Kraus (2017), who stated:

> User education and awareness might help to mitigate this threat. Thereby user education should address two factors: first, education regarding to security and privacy threats that may arise from apparently benign services or applications. For example, there are already tools for user education available such as anti-phishing education apps [29]. Second, education should also target awareness regarding security and privacy

> mechanisms that users may employ to protect their devices from such threats. (2017, 65, 66)

Additionally, several scholars have addressed specifically the need for mobile privacy education and awareness. I already reviewed some of them in the chapter 3 (see Park and Mo Jang 2014; Cushon 2013; Cyrus and Baggett 2012). For example, Park and Mo already called for support from the FCC on governmentally funded digital literacy training, awareness campaigns and/or standardization for privacy policies. Furthermore Koloseni (2015) recommends that "higher learning institutions need to conduct information security and privacy awareness campaigns and incorporate information security awareness as a topic or subtopic in order to prepare students on basic issues to adhere to when using social networks and mobile devices for learning" (2015, 116).

As a former academic librarian, I believe that libraries, librarians, and information science practitioners and scholars are in a unique position to play an integral part in this education. In the introduction of this study, I have already drawn attention to privacy education and libraries' involvement (see chapter 1). The unique chance for these stakeholders is further supported by a study from 2014 about the user's intention and attitude to use privacy tools on Facebook:

> The findings of our study also offer useful insights for practitioners. The results suggest that schools, colleges, and public libraries should develop appropriate awareness programs and training interventions to reinforce individuals' beliefs related to information resource safety, information resource vulnerability, privacy concern, threat severity, privacy intrusion, work impediment, and intrinsic cost associated with the use of privacy controls. (Taneja, Vitrano, and Gengo 2014, 172)

Some findings in this study, such as from chapter Mobile Privacy Settings Behavior and Management point toward the need for more education, especially when it comes to mobile devices, including IoT and wearable devices as well as phones and tablets. However, although the literature on mobile privacy education and awareness is sparse (see for example (Havelka and Lerski 2017), and information science and libraries professionals as well as scholars are in a unique position to provide mobile privacy education and start mobile awareness project on both sides of the Atlantic.

While this study is scholarly, I consider the recent developments in the mainstream media are also having a positive impact on the privacy education and awareness of society at large.

Here I observe especially shift in the US media, with major publications such as *The Washington Post*, and *The New York Times* leading the way in privacy awareness and education.

10.2.4.2 Cultural Comparative Summary

I only discern similarities and no differences for the privacy education theme.

10.3 Mobile Security

10.3.1 Similar Aspects German and American Students

Mixing and bringing up mobile security instead of mobile privacy is an occurrence I already observed and discussed in Fieldwork 1. Not surprisingly, I notice this phenomenon again in Fieldwork 2 – this time for a participant from each culture.

When it comes to the German participant, one possible explanation could be the German language. While privacy is called *"Privatsphäre"* or *"Privatheit"*, data privacy, and mobile privacy, both are called *"Datenschutz"* and *"mobiler Datenschutz*." The word *"Schutz"* means security in the German language.

When it comes to the American participant, I do not have a real explanation besides of what I have already discussed in the literature chapter or in discussion on Fieldwork 1.

10.3.2 Cultural Comparative Summary

While the topic does not pertain to this study's focus and research question I do identify confusion between privacy and security as well as mobile privacy and mobile security in both cultures, thus indeed, this phenomenon warrants more investigation. I will address this further in chapter 13.

10.4 Linguistic Highlights

10.4.1 Similar Aspects between Attitude German and American Students

In Fieldwork 2, I observe again in participants expressions what I call in mobile privacy complacency or its more severe form – what I call mobile privacy learned helplessness.

Beate, for example, uses words like:

Well, my ass [laughing]	***(verarschen kann ich mich auch selber [sie lacht laut]*)**
Pact with the devil	***(Pakt mit dem Teufel*)**

Or Jörg uses:

Fucked up	***(Scheiße gebaut*)**
I felt myself obliged	***(habe ich mich genötigt gefühlt)***

The two US participants illustrate with their languages similarly mobile privacy complacency. Steve for example says:

Threatening overinflated self-importance that makes people not like Facebook more

or him emphasizing:

It is basically I DO try to keep conscious of what sites I visit, what I click on

Ava expression expresses similar feelings such as:

Kind of trick you in mobile devices to get more information on you

or **Whose got the data [laughing] that is kind of scary [laughing]**

However, I will refrain from further discussion here, but refer back to chapter linguistic highlight and more specifically to 9.3.2 Cultural Comparative Summary.

10.4.2 Cultural Comparative Summary

Similar to Fieldwork 1's discussion I also do not perceive any cultural differences when it comes to linguistics.

10.5 Summary

In this chapter Fieldwork 2's findings have been discussed. The following chapter will answer the research question.

11. Summarized Discussion: Answering the Research Question

11.1 Overview

In the following chapter I summarize the discussion of Fieldwork 1 and 2 and most importantly I answer the research question:

Are there differences in the mobile privacy user behaviors and attitudes of American and German library and information science students?

11.2 Summarized Similarities and Differences

In the discussion for Fieldwork 1 and 2 I identify several themes where study participants **do not show at all** cultural differences in terms of mobile privacy behavior and attitude. These themes are

- privacy education
- privacy awareness/privacy protection
- mobile phone behavior

Even though German participants demonstrate specific behavior and attitude about WhatsApp and other messengers service I explain in the WhatsApp Behavior and Attitude - German Students chapter, why I believe this does not carry enough weight to justify a distinct cultural difference. Additionally, I find **no cultural differences** for

- Linguistic Highlights.

However, for most of the themes I find cultural differences and for many of these I find cultural differences either for German and/or American or both participants. Out of these I claim in the comparative cultural summary in discussion 1 and 2 **no** cultural difference for:

- privacy definition
- mobile privacy definition
- mobile privacy setting behavior and attitude
- Perfect Piano app experiment behavior and attitude
- app experiment favorite app behavior and attitude
- privacy policy attitude
- personal information and data attitude
- Facebook mobile privacy attitude and behavior

- GDPR

For some themes I find it difficult to determine cultural difference in terms of mobile privacy attitude and behavior. For these I would recommend further research:

- mobile phone attitude
- location service
- transparent human

Yet in the end I cautiously state that there are no cultural differences between German and American students here either.

The following table (Table 19) summarizes all themes and my conclusions in terms of mobile privacy behavior and attitude difference between US and German participants:

Themes	**Similarities (some/yes/ no/unclear)**	**Differences (German/US/ both/none)**	**Outcome in regard to research question**
mobile phone behavior	**some**	**German**	**no cultural difference**
mobile phone attitude	**unclear**	**both**	cautiously no, further research needed
linguistic highlights Fieldwork 1 and 2	**yes**	**none**	**no cultural differences**
privacy definition	**some**	**US**	**no cultural differences**
mobile privacy definition	**some**	**both**	**no cultural differences**
mobile privacy setting behavior and attitude	**some**	**US**	**no cultural differences**
location service	**some/unclear**	**German**	cautiously no, further research needed
Perfect Piano app experiment behavior and attitude	**some**	**US**	**no cultural difference**
app experiment favorite app behavior and attitude	**some**	**US**	**no cultural differences**
privacy policy attitude	**some**	**US**	**no cultural differences**

personal information and data attitude	**some**	**German**	**no cultural differences**
transparent human	**some/unclear**	**German**	cautiously no, further research needed
Facebook mobile privacy attitude and behavior	**some**	**German**	**no cultural difference**
GDPR	**some**	**both**	**no cultural differences**
privacy protection	**yes**	**none**	**no cultural differences**
privacy education	**yes**	**none**	**no cultural differences**

Table 19 Summary of all themes and conclusions in terms of mobile privacy behavior and attitude difference between US and German participants

This leads me to answering the research question:

Overall, I cannot find substantial differences in mobile privacy attitude and behavior between German and American library and information science students.

In conclusion I ask the question whether definitions I made in discussion 1 and 2 on mobile privacy behavior and or attitude, which are

- mobile privacy learned helplessness,
- mobile privacy complacency,
- mobile privacy pragmatism,
- mobile privacy objection,

although maybe not generalizable might be transferrable to other cultures in a globalized digital world? Hofstede, Hofstede, and Minkov (2010) contemplate similarly as the:

> Popular media often suggest that communication technologies, including television, e-mail, the Internet, mobile telephones, and social software, will bring people around the world together in a global village where cultural differences cease to matter. This dominance of technology over culture is an illusion. The software of the machines may be globalized, but the software of the minds that use them is not. (2010, 406)

Clearly these authors have not come to a decisive conclusion whether in today's globalized digital world and to bring it back to the research question mobile privacy behavior and attitude are different between cultures or if mobile privacy behavior and attitude is more and

more homogeneous around the world. But neither have I, though I certainly agree with what Trepte and Masur proclaim:

> There are more commonalities than differences. People all over the world think it is very important to protect their privacy in order to prevent privacy violations. Everybody consciously decides what to share and what not to share…At this point in time, it is unclear whether the current picture painted with this research is already a consequence of ongoing globalization or whether it represents a new globalized online culture. (2016, 71)

12. Research Limitations

Several limitations need to be noted regarding the present study.

1) The period of the data collection must be considered somewhat short, especially for an ethnographic study. As a counterbalance, the researcher was a perceptive ethnographer during her entire time in Berlin, Germany. She attended several classes at the Berlin School of Library and Information Science as guest editor, witnessed students' behavior and interaction with their smartphones in the library, and had several conversations with students who were not part of this study about the research topic. Furthermore, she observed Berlin's population, especially young adults, in their day-to-day life interactions with their smartphones, whether walking down the street, during train rides, in supermarkets, or other public places.

2) **Limitation of study participants** in terms of
   a. The relatively small number of students. However, since this is an ethnographic study, the goal was to illustrate a narrative based on qualitative findings. The researcher agrees with Lanclos's and Asher (2016) assertion that:

      > Ethnography should not be engaged in simply as a method that gives us more buckets of data to be sorted, visualized, and put into a report. Ethnography should be core to the business of the library. As praxis, practice informed by theory and ideology, it has the potential to transform libraries, librarianship, and indeed higher education. (2016, para. 28)

      Many ethnographic studies are small in sample size since the derived data is rich. The goal of this study is not to prove generalization of findings but instead to possibly confirm transferability to other scholars' findings.
   b. The relatively homogenous cultures studied. Even though the investigated cultures have some differences, one can consider them similar in many ways. This may have an impact on the result, and the following chapter on future research will address this issue.
   c. The participants are from two relatively elite schools and can be considered well educated and intellectually ambitious. The following chapter will also discuss this particular limitation.

3) The mobile privacy behavior on display was part of the interview and did not occur as part of students' natural environment and everyday life. It might, therefore, be considered simulated behavior that does not mirror students' behavior in the real world. This limitation will also be addressed in the chapter that follows.

13. Future Research Recommendations

This research has thrown up many questions in need of further investigation. Some of these questions are a direct result of the research limitations, while others came to mind during the overall dissertation process.

Possible areas for future research include:

1) Address limitations of study participants in terms of
    a. Comparison of less homogenous universities, for example a rural university in the US versus a more relatively elite university in Germany or vice versa
    b. Contrasting two countries that portray more significant differences according to Hofstede's dimensions, such as India or South Africa.
    c. Broadening the cultural scope of the investigation to include more than two countries. Here it would be interesting to include cultures from underrepresented regions such as Africa and South America.
    d. Comparing different age groups such as senior citizens versus teenagers.

2) Research mobile privacy behavior in real-time and in the natural environment of students. This could be, for example, similar to the methods of Smale and Regalado (2017), who:

    > Asked students to draw maps of their activities on a day they came to school. In contrast, other students created photo diaries of objects and locations related to academic work and scholarly habits ... To update our knowledge of how CUNY students move through their school days, we used text messaging to send prompts to students' cell phones throughout one day that asked them to report their location, activity, and affect, and subsequently interviewed students about their daily maps. (2017, 15,16)

3) Design and create qualitative usability studies about privacy policies.
    Throughout this study, the researcher discovered a lack of research on privacy policy using qualitative methods. Hence this area should be investigated further, especially considering that many participants came up with possible solutions on how to make privacy policy geared toward users and not as a legal safety measurement for companies. Furthermore, such a study should include interdisciplinary research and possibly include a real-world technology company.

4) Mobile security and mobile privacy:

In this study, mobile security came up as a phenomenon being confused quite frequently with mobile security. Hence this warrants further research using qualitative or mixed methodologies.

14. Conclusion

This thesis had the aim of exploring if there is a difference in mobile privacy behavior and attitude between American and German library and information science students. I intended to answer the research question by portraying a thick narrative that gave a voice to students from both cultures.

Overall, US and German information and library science students showed more similarities than differences in their behavior and attitude concerning mobile privacy. While I expected the German students to portray pro-privacy attitudes, I was surprised that American students' views about privacy, at least as an abstract concept, were on par. Even so, while the findings of this study are not generalizable, they do depict in both cultures an overall value for privacy as a right worth maintaining and preserving for in today's and future digital globalized world. Nonetheless, many students struggled with privacy as a concept as well as from a practical point of view. I discussed this conundrum in both the literature chapter and in the findings. It is certainly a topic to explore further from a globally digital-focused perspective.

Looking at mobile privacy, I feel the attitude and behavior in both nations paints a more somber picture. Here the confusion, learned helplessness, complacency, and/or pragmatism found among all participants illustrate a world where students (and as such consumers) seem to have no real choice in the matter. To requote the American participant Luke's thoughts on being or becoming a transparent human," *I cannot really have it any other way … Because in order to do what you want to usually do, … if you really want to get off the grid, you probably need to live in the jungle*." I detect this notion of having no real option to sustain mobile privacy as a smartphone user not only in the participants of this study, but also within myself, the ethnographic researcher.

Yet at the same time I see a small paradigm shift – more in the US than in Germany, which has always had stronger data privacy laws and a more pro-privacy attitude due to its fraught history – calling for stronger legal protections for consumers' personal information. Geoffrey A. Fowler from the Washington Post recently asserted, "with apologies to the Beastie Boys: You gotta fight for your right to privacy."(Fowler 2020a, para. 4) Furthermore, I, as a mobile privacy researcher, somewhat welcomed Facebook's/Cambridge Analytica data privacy

scandal in as much that it helped shine light on the topic of mobile privacy and data privacy. And as such, it created if not behavioral changes, at least more awareness on mobile privacy among all smartphones and app users. However, to support actual mobile privacy behavior change it seems that at least the options to become or be more mobile privacy conscious have increased. Here I would like to repeat for example Facebook's recent release of on improved *Privacy Checkup*[69] or the DuckDuckgo app[70].

I had chosen library and information science students as informants since a) privacy education is part of the curriculum in many information science departments, and b) current students grew up using mobile technologies. As such, they might have been exposed to mobile learning in their education. Yet as the findings and discussion have shown, I observe a need for improvement on mobile privacy education and awareness – on both sides of the Atlantic. As a researcher, former academic librarian, and hopefully future educator, I believe that current and future generations of librarians and information science professionals should play an integral part in educating their constituents and the broader digital global society on all issues pertaining to mobile privacy. Awareness and education can create change – a change where privacy, and particularly mobile privacy will remain a fundamental part of democracy, society, and humankind.

Yet, education and awareness are just one part of the equation – the other part has to be a collaborative effort and a dialogue between tech companies, information and library sciences as well as interdisciplinary research such as law, computer science and/or psychology.

In addition to future research recommendations, this study has made three contributions to the scholarly literature.

[69] https://about.fb.com/news/2020/01/privacy-checkup/

[70] https://duckduckgo.com/app

First: This is one of few qualitative studies using ethnographic methods to research intercultural mobile privacy behavior and attitude. And it might lay groundwork for future research or provided a framework for future research projects.

Second: Mobile privacy as a research topic is of value to more than information science scholars, and the qualitative nature of these findings might be of interest to a larger interdisciplinary research community.

Third: The findings and discussion validate the need for more privacy awareness projects and education in information science theory and practice.

References

"About This Study | Undergraduate Scholarly Habits Ethnography Project." n.d. Accessed September 25, 2018. https://ushep.commons.gc.cuny.edu/about-this-research/.

Acquisti, Alessandro. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification." In *EC '04: Proceedings of the 5th ACM conference on Electronic commerce*, 21–29. https://doi.org/10.1145/988772.988777.

admin. 2007. "Privacy Tool Kit." Text. Advocacy, Legislation & Issues. May 29, 2007. http://www.ala.org/advocacy/privacy/toolkit.

Aïmeur, Esma, Oluwa Lawani, and Kimiz Dalkir. 2016. "When Changing the Look of Privacy Policies Affects User Trust: An Experimental Study." *Computers in Human Behavior* 58 (May): 368–79. https://doi.org/10.1016/j.chb.2015.11.014.

Aisch, Gregor, Larry Buchanan, Amanda Cox and Kevin Quealy. 2017. "Economic Diversity and Student Outcomes at Rutgers." *The New York Times*, January 18, 2017, sec. The Upshot. https://www.nytimes.com/interactive/projects/college-mobility/rutgers-university.

Albrecht, Jan Philipp. 2016. "How the GDPR Will Change the World." *Eur. Data Prot. L. Rev.* 2: 287.

Allen, Anita L. 1998. "Coercing Privacy." *Wm. & Mary L. Rev.* 40: 723.

Almuhimedi, Hazim, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. "Your Location Has Been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 787–96. https://doi.org/10.1145/2702123.2702210.

Altman, Irwin. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Monterey, Calif: Brooks/Cole Pub. Co.

———. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues* 33 (3): 66–84.

"Annual Number of Mobile App Downloads Worldwide from 2016 to 2019 | Statista." 2020. January 2020. https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/.

"App Developers Are Tracking Kids despite Laws to Protect Their Privacy." 2014. PBS NewsHour. December 8, 2014. https://www.pbs.org/newshour/nation/app-developers-tracking-kids-despite-laws-protect-privacy.

Arkko, Jari, Charles E. Perkins, and David B. Johnson. n.d. "Mobility Support in IPv6." Accessed February 8, 2020. https://tools.ietf.org/html/draft-ietf-mext-rfc3775bis-08.

"Art. 4 GDPR – Definitions." n.d. *General Data Protection Regulation (GDPR)* (blog). Accessed October 20, 2019. https://gdpr-info.eu/art-4-gdpr./.

Arzola, Rebecca, and Stefanie Havelka. 2016. "Apps in Higher Education: Criteria and Evaluation." *The Charleston Advisor* 17 (3): 55–57. https://doi.org/10.5260/chara.17.3.55.

Asher, Andrew D., Susan Miller, and David Green. 2012. "Ethnographic Research in Illinois Academic Libraries: The ERIAL Project." *College Libraries and Student Culture: What We Now Know*, 1–14.

Asher, Andrew, and Susan Miller. 2011. "So You Want to Do Anthropology in Your Library." *Or a Practical Guide to Ethnographic Research in Academic Libraries*. http://www.erialproject.org/wp-content/uploads/2011/03/Toolkit-3.22.11.pdf

"The Diffusion of iPhones as a Learning Process | Asymco." November 6, 2013. http://www.asymco.com/2013/11/06/the-diffusion-of-iphones-as-a-learning-process/.

Au, M.H., and K.-K.R. Choo. 2017. "Mobile Security and Privacy." In *Mobile Security and Privacy: Advances, Challenges and Future Research Directions*, 1–4. Elsevier. https://doi.org/10.1016/B978-0-12-804629-6.00001-8.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center: Internet, Science & Tech (blog).* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Bambauer, Derek E. 2013. "Privacy versus Security." *J. Crim. L. & Criminology* 103: 667. https://www.jstor.org/stable/43895376.

Barkhuus, Louise, and Anind K. Dey. 2003. "Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns." In *Interact*, 3:702–12. Citeseer. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.527&rep=rep1&type=pdf.

Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Monday* 11 (9). https://doi.org/10.5210/fm.v11i9.1394.

Barth, Susanne, and Menno D.T. de Jong. 2017. "The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review." *Telematics and Informatics* 34 (7): 1038–58. https://doi.org/10.1016/j.tele.2017.04.013.

Baruh, Lemi, Ekin Secinti, and Zeynep Cemalcilar. 2017. "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis." *Journal of Communication* 67 (1): 26–53. https://doi.org/10.1111/jcom.12276.

Bauer, Christine, Jana Korunovska, and Sarah Spiekermann. 2012. "On the Value of Information-What Facebook Users Are Willing to Pay." *ECIS 2012 Proceedings*. https://aisel.aisnet.org/ecis2012/197/.

Beckwith, Richard. 2003. "Designing for Ubiquity: The Perception of Privacy." *IEEE Pervasive Computing* 2 (2): 40–46.

Bélanger, France, and Robert E. Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4): 1017–1042.

Bell, Judith. 2006. *Doing Your Research Project: A Guide for First-Time Researchers in Education, Health and Social Science.* 4th ed. Maidenhead, Berkshire, England: Open University Press.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20 (5): 313–24. https://doi.org/10.1080/01972240490507956.

Benjamin, Garfield. 2017. "Privacy as a Cultural Phenomenon." *Journal of Media Critiques* 3 (10): 55-74. https://www.ceeol.com/search/article-detail?id=697052.

Bennett, Sue. 2012. "Digital Natives." In *Encyclopedia of Cyber Behavior*, edited by Zheng Yan, 1:212–19. Hershey, PA: Information Science Reference.

Beres, Damon. 2014. "You Think Facebook Privacy Is Bad? Take A Look At Smartphone Games." *Huffington Post*, November 11, 2014, sec. Tech. https://www.huffingtonpost.com/2014/11/11/app-privacy_n_6139556.html.

Bhattacharya, Himika. 2008. "Empirical research." In *The SAGE Encyclopedia of Qualitative Research Methods 1, edited by Lisa M. Given,* 253-255.

Biswas, Debmalya, Imad Aad, and Gian Paolo Perrucci. 2013. "Privacy Panel: Usable and Quantifiable Mobile Privacy." In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference On*, 218–23. IEEE. https://boris.unibe.ch/45087/1/aad2.pdf.

Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius. 2018a. "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data." *Communication Research*. https://doi.org/10.1177/0093650218800915.

———. 2018b. "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data."*Communication Research*, https://doi.org/10.1177/0093650218800915.

Boshell, Paige. 2018. "Survey of Developments in Federal Privacy Law."*The Business Lawyer* 74 (1): 191–203.

Brandtzaeg, Petter Bae, Antoine Pultier, and Gro Mette Moen. 2018. "Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy." *Social Science Computer Review* 37 (4): 466–88. https://doi.org/10.1177/0894439318777706.

Braun, Max, and Sabine Trepte. 2018. "Privatheit Und Informationelle Selbstbestimmung. Trendmonitor Zu Den Einstellungen, Meinungen Und Perspektiven Der Deutschen." https://medienpsychologie.uni-hohenheim.de/fileadmin/einrichtungen/psych/Dateien/Laufende_Projekte/Trendmonitor_Privatheit_Hohenheim.pdf.

Brewster, Thomas. 2016. "You Have 30 Days To Stop WhatsApp Sharing Your Data With Facebook." Forbes. Accessed November 10, 2018. https://www.forbes.com/sites/thomasbrewster/2016/08/25/whatsapp-facebook-share-your-number-and-usage-data/.

Brown, Barry. 2001. "Studying the Internet Experience." *HP Laboratories Technical Report HPL* 49: 1–23. https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Calderón, Pablo Palma. 2017. *Datenschutz in Sozialen Netzwerken in Europa, Deutschland Und Chile*. Peter Lang International Academic Publishers.

Cao, Jinwei, and Andrea Everard. 2008. "User Attitude towards Instant Messaging: The Effect of Espoused National Cultural Values on Awareness and Privacy." *Journal of Global Information Technology Management* 11 (2): 30–57.

Chaffey, Dave. 2018. "Mobile Marketing Statistics 2018." Smart Insights. April 24, 2018. http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

"Children's Online Privacy Protection Rule ('COPPA')." 2013. Federal Trade Commission. July 25, 2013. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

Chin, Erika, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. "Measuring User Confidence in Smartphone Security and Privacy." In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1-16. https://dl.acm.org/doi/pdf/10.1145/2335356.2335358.

Cho, Hichang, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. "A Multinational Study on Online Privacy: Global Concerns and Local Responses." *New Media & Society* 11 (3): 395–416. https://doi.org/10.1177/1461444808101618.

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung. 2018. "The Role of Privacy Fatigue in Online Privacy Behavior." *Computers in Human Behavior* 81 (April): 42–51. https://doi.org/10.1016/j.chb.2017.12.001.

Christl, Wolfie, and Sarah Spiekermann. 2016. *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: Facultas.

Cohen, Tobi. 2018. "Educating Kids About Digital Privacy." EdCan Network. November 28, 2018. https://www.edcan.ca/articles/educating-kids-about-digital-privacy/.

CollegeSimply. n.d. "CUNY Lehman College Diversity & Student Demographics." CollegeSimply. Accessed January 26, 2020. https://www.collegesimply.com/colleges/new-york/cuny-lehman-college/students/.

"Complacency | Definition in the Cambridge English Dictionary." n.d. Accessed January 19, 2020. https://dictionary.cambridge.org/us/dictionary/english/complacency.

Copland, Fiona, and Angela Creese. 2015. "Linguistic Ethnography." In *Linguistic Ethnography: Collecting, Analysing and Presenting Data*, 12–28. 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications Ltd. https://doi.org/10.4135/9781473910607.

Correia, John, and Deborah Compeau. 2017. "Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA." In *Proceedings of the 50th Hawaii International Conference on System Sciences*: 4021–4030 http://128.171.57.22/bitstream/10125/41646/paper0497.pdf.

Couldry, Nick, and Jun Yu. 2018. "Deconstructing Datafication's Brave New World." *New Media & Society* 20 (12): 4473–91. https://doi.org/10.1177/1461444818775968.

"Country Comparison Germany and USA." 2019. Hofstede Insights. 2019. https://www.hofstede-insights.com/country-comparison//germany,the-usa/.

Crabtree, Andy, Tom Lodge, James Colley, Chris Greenhalgh, Richard Mortier, and Hamed Haddadi. 2016. "Enabling the New Economic Actor: Data Protection, the Digital Economy, and the Databox." *Personal and Ubiquitous Computing* 20 (6): 947–57. https://doi.org/10.1007/s00779-016-0939-3.

Cushon, Kate. 2013. "An Education in Privacy: Best Practices for Academic Libraries in the Age of Social Media." *In M-Libraries* 4, edited by Ally, Mohamed, Needham, Gill: 91–99.

Cyrus, John W. W., and Mark P. Baggett. 2012. "Mobile Technology: Implications for Privacy and Librarianship." *The Reference Librarian* 53 (3): 284–96. https://doi.org/10.1080/02763877.2012.678765.

"Data Privacy Project." n.d. Data Privacy Project. Accessed August 3, 2018. https://dataprivacyproject.org/.

Davazdahemami, Behrooz, Bryan Hammer, and Amr Soror. 2016. "Addiction to Mobile Phone or Addiction through Mobile Phone?" In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 1467–76. IEEE.

"DBT_2015_05_29_Datenschutz_in_Bibliotheken_endg. Pdf." n.d. Accessed July 24, 2018. https://www.bibliotheksverband.de/fileadmin/user_upload/DBV/aktuelles/DBT_2015_05_29_Datenschutz_in_Bibliotheken_endg.pdf.

De Luca, Alexander, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. "Expert and Non-Expert Attitudes towards (Secure) Instant Messaging." In *Twelfth Symposium on Usable Privacy and Security {SOUPS}*: 147–57. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-de-luca.pdf.

dempsey. 2008. "M-Libraries." *Lorcan Dempsey's Weblog* (blog). November 12, 2008. http://orweblog.oclc.org/m-libraries/.

Dienlin, Tobias. 2014. "The Privacy Process Model." *Medien Und Privatheit*, 105–22.

"Directive 2002/58/EC of the European Parliament and of the C... - EUR-Lex." n.d. Accessed January 17, 2020. https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32002L0058.

Dogruel, Leyla, Sven Joeckel, and Jessica Vitak. 2017. "The Valuation of Privacy Premium Features for Smartphone Apps: The Influence of Defaults and Expert Recommendations." *Computers in Human Behavior* 77 (December): 230–39. https://doi.org/10.1016/j.chb.2017.08.035.

Downes, Larry. 2018. "How More Regulation for U.S. Tech Could Backfire." *Harvard Business Review*, February 9, 2018. https://hbr.org/2018/02/how-more-regulation-for-u-s-tech-could-backfire.

Dresing, Thorsten, Thorsten Pehl, and Christian Schmieder. 2015. "Manual (on) Transcription: Transcription Conventions, Software Guides and Practical Hints for Qualitative Researchers." *Marburg: Self-Published.*

D'Souza, Giles, and Joseph E Phelps. 2009. "The Privacy Paradox: The Case of Secondary Disclosure." *Review of Marketing Science* 7 (1). https://doi.org/10.2202/1546-5616.1072.

Emami-Naeini, Pardis, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–12. Glasgow, Scotland Uk: ACM Press. https://doi.org/10.1145/3290605.3300764.

"ERIAL Project." 2020. Accessed September 25, 2018. http://www.erialproject.org/.

Erlingsson, Christen, and Petra Brysiewicz. 2013. "Orientation among Multiple Truths: An Introduction to Qualitative Research." *African Journal of Emergency Medicine* 3 (2): 92–99. https://doi.org/10.1016/j.afjem.2012.04.005.

Ermakova, Tatiana, Annika Baumann, Benjamin Fabian, and Hanna Krasnova. 2014. "Privacy Policies and Users' Trust: Does Readability Matter?" https://boris.unibe.ch/68895/.

European Union, and Agency for Network and Information Security. 2017. *Privacy and Data Protection in Mobile Applications: A Study on the App Development Ecosystem and the Technical Implementation of GDPR.* http://dx.publications.europa.eu/10.2824/114584.

Fefer, Rachel F. 2019. "Data Flows, Online Privacy, and Trade Policy." *Congressional Research Service*, March, 25. https://fas.org/sgp/crs/row/R45584.pdf.

Fefer, Rachel F, and Kristin Archick. 2019. "EU Data Protection Rules and U.S. Implications." *Congressional Research Service*, August, 2. https://fas.org/sgp/crs/row/IF10896.pdf.

Fetterman, David M. 2010. *Ethnography: Step-by-Step*. 3rd ed. Applied Social Research Methods Series 17. Los Angeles: SAGE.

Fisher, Drew, Leah Dorner, and David Wagner. 2012. "Short Paper: Location Privacy: User Behavior in the Field." In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 51–56. ACM. https://doi.org/10.1145/2381934.2381945.

Flick, Uwe. 2009. *An Introduction to Qualitative Research*. 4th ed. Los Angeles: Sage Publications.

Foster, Nancy Fried, and Susan Gibbons, eds. 2007. *Studying Students: The Undergraduate Research Project at the University of Rochester*. Chicago: Association of College and Research Libraries.

Fowler, Geoffrey A. 2020a. "Perspective | Don't Sell My Data! We Finally Have a Law for That." Washington Post. 2020. https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/.

———. 2020b. "Perspective | Facebook Will Now Show You Exactly How It Stalks You — Even When You're Not Using Facebook." Washington Post. January 29, 2020.

https://www.washingtonpost.com/technology/2020/01/28/off-facebook-activity-page/.

Freude, A, and T Freude. 2016. "Echos of History: Understanding German Data Protection." *Bertelsmann Foundation*. http://bfna.insomnation.com/research/echos-of-history-understanding-german-data-protection/.

Geertz, Clifford. 1973. *The Interpretation of Cultures*. Basic books.

General Assembly. 2016. "United Nations Official Document." The Right to Privacy in the Digital Age. November 16, 2016. https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1.

Gerber, Nina, Benjamin Reinheimer, and Melanie Volkamer. 2019. "Investigating People's Privacy Risk Perception." *Proceedings on Privacy Enhancing Technologies* 2019 (3): 267–88. https://doi.org/10.2478/popets-2019-0047.

"Germany: Smartphone User Penetration 2015-2022." 2020. Statista. 2020. http://www.statista.com/statistics/568095/predicted-smartphone-user-penetration-rate-in-germany/.

Giebels, Ellen, Miriam S. D. Oostinga, Paul J. Taylor, and Joanna L. Curtis. 2017. "The Cultural Dimension of Uncertainty Avoidance Impacts Police–Civilian Interaction." Law and Human Behavior 41 (1): 93–102. https://doi.org/10.1037/lhb0000227.

Ginosar, Avshalom, and Yaron Ariel. 2017. "An Analytical Framework for Online Privacy Research: What Is Missing?" *Information & Management* 54 (7): 948–57. https://doi.org/10.1016/j.im.2017.02.004.

Given, Lisa M., ed. 2008. "Ethnography." In *The SAGE Encyclopedia of Qualitative Research Methods*, 1:288–92. Thousand Oaks, CA: SAGE Publications.

Gkioulos, Vasileios, Gaute Wangen, Sokratis Katsikas, George Kavallieratos, and Panayiotis Kotzanikolaou. 2017. "Security Awareness of the Digital Natives." *Information* 8 (2): 42. https://doi.org/10.3390/info8020042.

Goodman, Valeda Dent. 2011. "Applying Ethnographic Research Methods in Library and Information Settings." *Libri* 61 (1): 1–11. https://doi.org/10.1515/libr.2011.001.

Gullion, Jessica Smartt. 2016. *Writing Ethnography.* Rotterdam: SensePublishers.

Harms, Johannes, Martina Kratky, Christoph Wimmer, Karin Kappel, and Thomas Grechenig. 2015. "Navigation in Long Forms on Smartphones: Scrolling Worse than Tabs, Menus, and Collapsible Fieldsets." In *Human-Computer Interaction – INTERACT 2015*, edited by Julio Abascal, Simone Barbosa, Mirko Fetter, Tom Gross, Philippe Palanque, and Marco Winckler, 333–40. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-22698-9_21.

Hartmann, Maren. 2011. "Mobile Privacy: Contexts." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte, Sabine and Reinecke, Leonard, 191–203. Springer.

Havelka, Stefanie. 2013. "Mobile Information Literacy: Supporting Students' Research and Information Needs in a Mobile World." *Internet Reference Services Quarterly* 18 (3–4): 189–209. https://doi.org/10.1080/10875301.2013.856366.

Havelka, Stefanie, and Martha Lerski. 2017. "Privacy Initiatives at The City University of New York (CUNY)." In *Protecting Patron Privacy: A LITA Guide.*, edited by Bobbi L. Newman and Bonnie Tijerina, 117–28. Lanham, MD: Rowman & Littlefield.

Head, Alison Jane, Barbara Fister, and Margy MacMillan. 2020. "Information Literacy in the Age of Algorithms." PROJECT INFORMATION L. https://www.projectinfolit.org/uploads/2/7/5/4/27541717/final_algo_study_report_2020-01-14.pdf.

Heizereder, Steffen. 2015. "Der Gläserne Mensch." *Forum Für Bibliothek Und Information* 67 (11): 649.

Heller, Monica. 2009. "Doing Ethnography." In *The Blackwell Guide to Research Methods in Bilingualism and Multilingualism*, edited by Li Wei and Melissa G. Moyer, 249–62. Oxford, UK: Blackwell Publishing Ltd. https://doi.org/10.1002/9781444301120.ch14.

Henke, Jakob, Sven Joeckel, and Leyla Dogruel. 2018. "Processing Privacy Information and Decision-Making for Smartphone Apps among Young German Smartphone Users." *Behaviour & Information Technology* 37 (5): 488–501. https://doi.org/10.1080/0144929X.2018.1458902.

Hillman, Serena, and Carman Neustaedter. 2017. "Trust and Mobile Commerce in North America." *Computers in Human Behavior* 70 (May): 10–21. https://doi.org/10.1016/j.chb.2016.12.061.

Hofstede, Geert. 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*. Sage publications.

———. 2011. "Dimensionalizing Cultures: The Hofstede Model in Context." *Online Readings in Psychology and Culture* 2 (1). https://doi.org/10.9707/2307-0919.1014.

Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. 1991. "Cultures and Organizations: Intercultural Cooperation and Its Importance for Survival." *Software of the Mind London: McGraw-Hill*.

Hofstede, Geert, and Michael Minkov. 2010. "Long- versus Short-Term Orientation: New Perspectives." *Asia Pacific Business Review* 16 (4): 493–504. https://doi.org/10.1080/13602381003637609.

Hoofnagle, Chris Jay, Jennifer King, Su Li, and Joseph Turow. 2010. "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?" 1–20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

Hull, Gordon. 2015. "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17 (2): 89–101. https://doi.org/10.1007/s10676-015-9363-z.

"HUMAN INFORMATION BEHAVIOR | Courses | School of Communication and Information | Rutgers University." 2019. HUMAN INFORMATION BEHAVIOR. 2019. https://comminfo.rutgers.edu/academics/courses?courses=Human+Information+behavior&program=32.

"IFLA Statement on Privacy in the Library Environment" n.d. Accessed July 31, 2018. https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf.

"Infographic-Gdpr_in_numbers_1.Pdf." n.d. Accessed February 2, 2020. https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.

"INFORMATION POLICY | Courses | School of Communication and Information | Rutgers University." 2019. INFORMATION POLICY. 2019. https://comminfo.rutgers.edu/academics/courses/32?courses=Information+Policy+&program=All#course-271.

"iPhone App Store Downloads Top 10 Million in First Weekend." 2008. Apple Newsroom. July 14, 2008. https://www.apple.com/newsroom/2008/07/14iPhone-App-Store-Downloads-Top-10-Million-in-First-Weekend/.

Jain, Anurag Kumar, and Devendra Shanbhag. 2012. "Addressing Security and Privacy Risks in Mobile Applications." *IT Professional* 14 (5): 28–33. https://ieeexplore.ieee.org/document/6243128.

Jarzabkowski, Paula, Rebecca Bednarek, and Jane K Lê. 2014. "Producing Persuasive Findings: Demystifying Ethnographic Textwork in Strategy and Organization Research." *Strategic Organization* 12 (4): 274–87. https://doi.org/10.1177/1476127014554575.

Joeckel, Sven, Leyla Dogruel, and Nicholas David Bowman. 2017. "The Reliance on Recognition and Majority Vote Heuristics over Privacy Concerns When Selecting Smartphone Apps among German and US Consumers." *Information, Communication & Society* 20 (4): 621–36. https://doi.org/10.1080/1369118X.2016.1202299.

Jones, Tessa. 2014. "Students' Cell Phone Addiction and Their Opinions." *Elon J Undergrad Res Commun* 5 (1): 74–80. http://www.elon.edu/docs/e-web/academics/communications/research/vol5no1/08jonesejspring14.pdf.

Khan, Lina M. 2019. "THE SEPARATION OF PLATFORMS AND COMMERCE." *Columbia Law Review* 119 (4): 973–1098. www.jstor.org/stable/26632275.

Khoo, Michael, Lily Rozaklis, and Catherine Hall. 2012. "A Survey of the Use of Ethnographic Methods in the Study of Libraries and Library Users." *Library & Information Science Research* 34 (2): 82–91. https://doi.org/10.1016/j.lisr.2011.07.010.

King, Jennifer. 2012. "How Come I'm Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2493412.

Kokolakis, Spyros. 2017. "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon." *Computers & Security* 64 (January): 122–34. https://doi.org/10.1016/j.cose.2015.07.002.

Koloseni, Daniel. 2015. "Security, Privacy Awareness vs. Utilization of Social Networks and Mobile Apps for Learning: Students Preparedness." *Advances in Computer Science: An International Journal* 4 (3): 111–17.

König, Pascal D. 2017. "The Place of Conditionality and Individual Responsibility in a 'Data-Driven Economy.'" *Big Data & Society* 4 (2): 1–14. https://doi.org/10.1177/2053951717742419.

Koohikamali, Mehrdad. 2016. "THREE ESSAYS ON INFORMATION PRIVACY OF MOBILE USERS IN THE CONTEXT OF MOBILE APPS." PhD diss., Denton, Texas: University of North Texas.

Krasnova, Hanna, and Natasha F Veltri. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA." In *43rd Hawaii international conference on system sciences:* 1-10. IEEE.

Krasnova, Hanna, and Natasha F Veltri. 2011. "Behind the Curtains of Privacy Calculus on Social Networking Sites: The Study of Germany and the USA." In *10th international conference on Wirtschaftsinformatik, Zurich, Switzerland,* 891–900.

Krasnova, Hanna, Natasha F. Veltri, and Oliver Günther. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus." *Business & Information Systems Engineering* 4 (3): 127–35. https://doi.org/10.1007/s12599-012-0216-6.

Kraus, Lydia. 2017. "User Experience with Mobile Security and Privacy Mechanisms." Technische Universität Berlin. Doctoral Thesis, Berlin: Technische Universität Berlin. https://doi.org/10.14279/depositonce-6029.

Krenske, Leigh. 2002. "You're Researching What?' The Importance of Self in Ethnographic Research." *Qualitative Research in Practice: Examples for Discussion and Analysis. San Francisco, CA: Jossey-Bass*, 262–285.

Kuckartz, Udo, and Anne McWhertor. 2014. *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. Los Angeles: SAGE.

Kununka, Sophia. 2018. "User Centric Privacy Policy Modelling." Doctoral Thesis, Manchester: University of Manchester. https://www.research.manchester.ac.uk/portal/files/102606682/FULL_TEXT.PDF.

Lanclos, Donna, and Andrew D. Asher. 2016. "'Ethnographish': The State of the Ethnography in Libraries." *Weave: Journal of Library User Experience* 1 (5). https://doi.org/10.3998/weave.12535642.0001.503.

Landau, Susan. 2013. "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security & Privacy* 11 (4): 54–63.

Lee, Jong-Moon, and Yoo-Seong Song. 2015. "Mobile Information-Seeking Behavior: A Comparative Study." *IFLA Journal* 41 (2): 153–61. https://doi.org/10.1177/0340035215583501.

Lesorogol, Carolyn K. 2005. "Experiments and Ethnography: Combining Methods for Better Understanding of Behavior and Change." *Current Anthropology* 46 (1): 129–36. https://doi.org/10.1086/427099.

Li, Qing, and Greg Clark. 2013. "Mobile Security: A Look Ahead." *IEEE Security & Privacy* 11 (1): 78–81. https://doi.org/10.1109/MSP.2013.15.

"Library Freedom Project – Making Real the Promise of Intellectual Freedom in Libraries." n.d. Accessed August 3, 2018. https://libraryfreedomproject.org/.

Lim, Soo Ling, Peter Bentley, Natalie Kanakam, Fuyuki Ishikawa, and Shinichi Honiden. 2015. "Investigating Country Differences in Mobile App User Behavior and Challenges for Software Engineering." *IEEE Transactions on Software Engineering*, 41 (1): 40-64. https://doi.org/10.1109/TSE.2014.2360674.

Lin, Jialiu, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing." In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 501–10. ACM. https://doi.org/10.1145/2370216.2370290.

Lin, Jialiu, Bin Liu, Norman Sadeh, and Jason I. Hong. 2014. "Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings." *In 10th Symposium On Usable Privacy and Security ({SOUPS} 2014): 199-212.* https://www.usenix.org/system/files/conference/soups2014/soups14-paper-lin.pdf.

LLC, SnoopWall. n.d. "SnoopWall Launches Free Privacy App to Detect and Block Cyber Criminals, Snoops, Spies and Online Predators." Accessed November 14, 2018. https://www.prnewswire.com/news-releases/snoopwall-launches-free-privacy-app-to-detect-and-block-cyber-criminals-snoops-spies-and-online-predators-270328291.html.

Lopez-Fernandez, Olatz, Daria J. Kuss, Lucia Romo, Yannick Morvan, Laurence Kern, Pierluigi Graziani, Amélie Rousseau, et al. 2017. "Self-Reported Dependence on Mobile Phones in Young Adults: A European Cross-Cultural Empirical Survey." *Journal of Behavioral Addictions* 6 (2): 168–77. https://doi.org/10.1556/2006.6.2017.020.

Lutz, Christoph, and Pepe Strathoff. 2014. "Privacy Concerns and Online Behavior–Not so Paradoxical after All? Viewing the Privacy Paradox through Different Theoretical Lenses." *Viewing the Privacy Paradox Through Different Theoretical Lenses (April 15, 2014)*. http://dx.doi.org/10.2139/ssrn.2425132.

Maass, Peter, and Megha Rajagopalan. 2012. "Opinion | That's Not My Phone, It's My Tracker." *The New York Times*, July 13, 2012, sec. Sunday Review. https://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html.

Madrigal, Alexis C. 2018. "Even Amid Scandal, Facebook Is Unstoppable." The Atlantic. May 1, 2018. https://www.theatlantic.com/technology/archive/2018/05/facebook-the-unstoppable/559301/.

Maier, Steven F., and Martin E. P. Seligman. 2016. "Learned Helplessness at Fifty: Insights from Neuroscience." *Psychological Review* 123 (4): 349–67. https://doi.org/10.1037/rev0000033.

Manning, Peter K. 2001. "And Ethnography." Edited by Paul Atkinson. *Handbook of Ethnography*, Sage.

Martin, Kirsten E. 2013. "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online." *First Monday* 18 (12–2). https://firstmonday.org/ojs/index.php/fm/article/view/4838/3802.

McCormick, Rich. 2017. "Watch Steve Jobs Introduce the IPhone 10 Years Ago Today." The Verge. January 9, 2017. https://www.theverge.com/2017/1/9/14208974/iphone-announcement-10-year-anniversary-steve-jobs.

McDonald, Aleecia M., and Lorrie Faith Cranor. 2008. "The Cost of Reading Privacy Policies." *ISJLP* 4: 543. https://kb.osu.edu/handle/1811/72839.

Meade, Phillip T., and Luis Rabelo. 2004. "The Technology Adoption Life Cycle Attractor: Understanding the Dynamics of High-Tech Markets." *Technological Forecasting and Social Change* 71 (7): 667–84. https://doi.org/10.1016/j.techfore.2004.01.008.

Meso, Peter, Philip Musa, and Victor Mbarika. 2005. "Towards a Model of Consumer Use of Mobile Information and Communication Technology in LDCs: The Case of Sub-Saharan Africa." *Information Systems Journal* 15 (2): 119–46. https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2575.2005.00190.x?c.

Meyer, David. 2018. "IN PRIVACY WE TRUST. (Federal Data Privacy Law)." *Fortune* 178 (6): 38.

Miltgen, Caroline Lancelot, and Dominique Peyrat-Guillard. 2014. "Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries." *European Journal of Information Systems* 23 (2): 103–25. https://doi.org/10.1057/ejis.2013.17.

Mims, Christopher. 2018. "Your Location Data Is Being Sold--Often Without Your Knowledge; Location-Based Ads Are Growing, Which Means the Industry Has More Ways than Ever to Track You." *Wall Street Journal (Online)*, March 4, 2018.

Mohanty, Atasi, Rabindra Kumar Pradhan, and Lalatendu Kesari Jena. 2015. "Learned Helplessness and Socialization: A Reflective Analysis." *Psychology* 06 (07): 885–95. https://doi.org/10.4236/psych.2015.67087.

Molla, Rani. 2017. "How Apple's iPhone Changed the World: 10 Years in 10 Charts." Recode. June 26, 2017. https://www.recode.net/2017/6/26/15821652/iphone-apple-10-year-anniversary-launch-mobile-stats-smart-phone-steve-jobs.

Morey, Timothy, Theodore Forbath, and Allison Schoop. 2015. "Customer Data: Designing for Transparency and Trust." *Harvard Business Review* 93 (5): 96–105.

Moscato, Donald R., Shoshana Altschuller, and Eric D. Moscato. 2013. "Privacy Policies on Global Banks' Websites: Does Culture Matter?" *Communications of the IIMA* 13 (4): 7.

Mozilla. 2018. "We Asked People How They Feel About Facebook. Here's What They Said." Medium. May 8, 2018. https://medium.com/read-write-participate/we-asked-people-how-they-feel-about-facebook-heres-what-they-said-4a548dfeabd.

Muth, Max. Bayerischer Rundfunk. 2016. "Änderung bei Whatsapp: So verhindern Sie, dass Facebook Ihre Nummer für Werbung nutzt," https://www.br.de/nachricht/whatsapp-teilt-daten-mit-facebook-100.html.

Newman, Bobbi L., and Bonnie Tijerina, eds. 2017. "Privacy Law and Regulation." In *Protecting Patron Privacy: A LITA Guide*, by Zimmer, Michael and Caldwell-Stone, Deborah, 23–33. Library Information Technology Association (LITA) Guides. Lanham, Maryland: Rowman & Littlefield.

Nissenbaum, Helen. 2018. "Respecting Context to Protect Privacy: Why Meaning Matters." *Science and Engineering Ethics* 24 (3): 831–52. https://doi.org/10.1007/s11948-015-9674-9.

Nissenbaum, Helen Fay. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif: Stanford Law Books.

Nolen, Jeannette L. 2017. "Learned Helplessness" *Encyclopædia Britannica.* https://www.britannica.com/science/learned-helplessness.

Norberg, Patricia A, Daniel R Horne, and David A Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126.

"Number of Apps Available in Leading App Stores 2018 | Statistic." 2020. Statista. January 2020. http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

"Number of Smartphone Users in Germany from January 2009 to 2018." 2018. February 2018. https://www.statista.com/statistics/461801/number-of-smartphone-users-in-germany/.

"Number of Smartphone Users in the U.S. 2010-2023." 2019. Statista. February 2019. http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/.

"Number of Smartphone Users Worldwide 2014-2020." 2019. Statista. September 2019. http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2018. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23 (1): 128–47. https://doi.org/10.1080/1369118X.2018.1486870.

Oberlies, Mary K. 2015. "Techniques for Finding and Evaluating Great Library Apps." *Online Searcher*, 2015. Academic OneFile.

Olmstead, Kenneth, and Aaron Smith. 2017. "Americans and Cybersecurity." *Pew Research Center* 26.

Olson, Michael A. 2007. "MODE Model." In *Encyclopedia of Social Psychology*, edited by Roy F. Baumeister and Kathleen D. Vohs, 2:584–86. Thousand Oaks, CA: SAGE Publications.

Omrani, Nessrine, and Nicolas Soulié. 2017. "Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM." https://econpapers.repec.org/RePEc:zbw:itsp17:168531.

O'Reilly, Karen. 2012. *Ethnographic Methods*. Routledge.

Palmer, Vernon Valentine. 2011. "Three Milestones in the History of Privacy in the United States." *Tul. Eur. & Civ. LF* 26: 67.

Park, Yong Jin. 2013. "Digital Literacy and Privacy Behavior Online." *Communication Research* 40 (2): 215–36. https://doi.org/10.1177/0093650211418338.

Park, Yong Jin, and S. Mo Jang. 2014. "Understanding Privacy Knowledge and Skill in Mobile Communication." *Computers in Human Behavior* 38 (September): 296–303. https://doi.org/10.1016/j.chb.2014.05.041.

Pentina, Iryna, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. "Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison." *Computers in Human Behavior* 65 (December): 409–19. https://doi.org/10.1016/j.chb.2016.09.005.

Perin, Andrew. 2018. "Americans Are Changing Their Relationship with Facebook." *Pew Research Center* (blog). September 5, 2018. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

"Player 3 Has Joined the Game – Chrome OS Detachable Tablets Paint a Brighter Future While Tablet Market Struggles, According to IDC." n.d. IDC: The Premier Global Market Intelligence Company. Accessed August 1, 2018. https://www.businesswire.com/news/home/20180503005395/en/Player-3-Joined-Game-%E2%80%93-Chrome-OS.

Ponterotto, Joseph G. 2006. "Brief Note on the Origins, Evolution, and Meaning of the Qualitative Research Concept Thick Description." *The Qualitative Report* 11 (3): 538–49.

"PrivacyGrade." n.d. Accessed November 10, 2018. http://privacygrade.org/.

"PrivacyProxy - Privacy Reimagined." n.d. Accessed November 14, 2018. http://www.privacyproxy.io/.

"Programs." 2018. *Choose Privacy Every Day* (blog). 2018. https://chooseprivacyeveryday.org/programs/.

Ramsden, Bryony. 2016. "Ethnographic Methods in Academic Libraries: A Review." *New Review of Academic Librarianship* 22 (4): 355–69. https://doi.org/10.1080/13614533.2016.1231696.

Raul, Alan Charles, and Mohan, Vivek K. 2018. "United States." In *The Privacy, Data Protection and Cybersecurity Law Review*, edited by Alan Charles Raul, 376–403.

Reay, Ian, Patricia Beatty, Scott Dick, and James Miller. "Privacy policies and national culture on the internet." Information Systems Frontiers 15, no. 2 (2013): 279-292

Regalado, Mariana, and Maura A. Smale. 2015. "'I Am More Productive in the Library Because It's Quiet': Commuter Students in the College Library." *College & Research Libraries* 76 (7): 899–913. https://doi.org/10.5860/crl.76.7.899.

Reinfelder, Lena, Zinaida Benenson, and Freya Gassmann. 2014. "Differences between Android and IPhone Users in Their Security and Privacy Awareness." In *International Conference on Trust, Privacy and Security in Digital Business*, 156–67. Springer.

"Revontulet Soft, Perfect Piano, Walk Band, Nora, Revontulet Studio." n.d. Accessed November 10, 2018. http://revontuletsoft.com/.

"Right to Be Informed." n.d. *General Data Protection Regulation (GDPR)* (blog). Accessed January 30, 2020. https://gdpr-info.eu/issues/right-to-be-informed/.

Rothgeb, Jennifer, M. 2008. "Pilot Test." In *Encyclopedia of Survey Research Methods*, edited by Paul Lavrakas. 2455 Teller Road, Thousand Oaks California 91320 United States of America: Sage Publications, Inc.

Salmona, Michelle, James Melton, and Robert Miller. 2013. "Online Social Networking across Cultures: An Exploration of Divergent and Common Practices." *Journal of Technical Writing and Communication* 43 (3): 317–31.

Sanday, Peggy Reeves. 1979. "The Ethnographic Paradigm(s)." *Administrative Science Quarterly* 24 (4): 527–538. https://doi.org/10.2307/2392359.

Sandstrom, Alan R., and Pamela Effrein Sandstrom. 1995. "The Use and Misuse of Anthropological Methods in Library and Information Science Research." *The Library Quarterly* 65 (2): 161–99.

Saylor, Michael. 2012. *The Mobile Wave: How Mobile Intelligence Will Change Everything*. 1st Vanguard Press ed. New York: Vanguard Press.

Sayre, Shay, and David Horne. 2000. "Trading Secrets for Savings: How Concerned Are Consumers about Club Cards as a Privacy Threat?" *in NA - Advances in Consumer Research Volume 27, eds. Stephen J. Hoch and Robert J. Meyer, Provo, UT: Association for Consumer Research, Pages: 151-155.* https://www.acrwebsite.org/volumes/8379/volumes/v27/NA-27.

Schaub, Florian, Rebecca Balebako, and Lorrie Faith. Cranor. 2017. "Designing Effective Privacy Notices and Controls." *IEEE Internet Computing* PP (99): 1–1. https://doi.org/10.1109/MIC.2017.265102930.

Schensul, Stephen L., Jean J. Schensul, and Margaret Diane LeCompte. 1999. *Essential Ethnographic Methods: Observations, Interviews, and Questionnaires*. Vol. 2. Rowman Altamira.

Schmuck, Peter, Tim Kasser, and Richard M. Ryan. 2000. "Intrinsic and Extrinsic Goals: Their Structure and Relationship to Well-Being in German and US College Students." *Social Indicators Research* 50 (2): 225–41.

Schulze, Matthias. 2015. "Patterns of Surveillance Legitimization. The German Discourse on the NSA Scandal." *Surveillance & Society* 13 (2): 197–217.

Schwab, Klaus, Alan Marcus, J. O. Oyola, William Hoffman, and Michele Luzi. 2011. "Personal Data: The Emergence of a New Asset Class." In *An Initiative of the World Economic Forum*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

Scoble, Robert, and Shel Israel. 2014. *Age of Context: Mobile, Sensors, Data and the Future of Privacy*. Patrick Brewster Press.

Seadle, Michael. 2000. "Project Ethnography: An Anthropological Approach to Assessing Digital Library Services." https://www.ideals.illinois.edu/bitstream/handle/2142/8338/librarytrendsv49i2j_opt.pdf?sequence=1.

Seale, Clive, and David Silverman. 1997. "Ensuring Rigour in Qualitative Research." *The European Journal of Public Health* 7 (4): 379–84.

Shambare, Richard, Robert Rugimbana, and Takesure Zhowa. 2012. "Are Mobile Phones the 21st Century Addiction?" *African Journal of Business Management* 6 (2): 573–77.

Sheth, Swapneel, Gail Kaiser, and Walid Maalej. 2014. "Us and Them: A Study of Privacy Requirements across North America, Asia, and Europe." In *Proceedings of the 36th International Conference on Software Engineering (ICSE 2014).* Association for Computing Machinery, New York, NY, USA, 859–870. https://doi.org/10.1145/2568225.2568244.

Shklovski, Irina, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use." In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, 2347–2356. CHI '14. New York, NY, USA: ACM. https://doi.org/10.1145/2556288.2557421.

Sigmund, Tomáš. 2017. "Ambiguous Character of Information Privacy and Its Possible Solution." *Journal of Information Ethics* 26 (2): 34–53.

Singer, Natasha. 2013. "Consumer Data Protection Laws, an Ocean Apart." *The New York Times*, February 2, 2013, sec. Technology. https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

Singh, Varun. Context-awareness: control over disclosure and privacy in a social environment. TKK technical reports in computer science and engineering, Helsinki University of Technology Department of Computer Science and Engineering. https://api.semanticscholar.org/CorpusID:4696899.

Singh, Tanuja, and Mark E Hill. 2003. "Consumer Privacy and the Internet in Europe: A View from Germany." *Journal of Consumer Marketing*.

Slavin, Rocky, Xiaoyin Wang, Mitra Bokaei Hosseini, James Hester, Ram Krishnan, Jaspreet Bhatia, Travis D. Breaux, and Jianwei Niu. 2016. "Toward a Framework for Detecting Privacy Policy Violations in Android Application Code." In *Proceedings of the 38th International Conference on Software Engineering*, 25–36. https://doi.org/10.1145/2884781.2884855.

Smale, Maura A., and Mariana Regalado. 2017. *Digital Technology as Affordance and Barrier in Higher Education*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-48908-7.

"Smartphone OS: Sales Market Share in Germany 2019." 2020. Statista. January 2020. https://www.statista.com/statistics/461997/smartphone-os-market-shares-of-sales-in-germany/.

"Smartphones in Germany." 2019. Statista. https://www.statista.com/study/39558/smartphones-in-germany-statista-dossier/.

"Smartphones in the U.S." 2018. https://www.statista.com/study/26643/smartphones-in-the-us-statista-dossier/.

Solove, Daniel J. 2007. "I've Got Nothing to Hide and Other Misunderstandings of Privacy." *San Diego L. Rev.* 44: 745.

Spensky, Chad, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay, Ari Trachtenberg, Rick Housley, and Robert K. Cunningham. 2016. "SoK: Privacy on Mobile Devices – It's Complicated." *Proceedings on Privacy Enhancing Technologies* 2016 (3): 96–116. https://doi.org/10.1515/popets-2016-0018.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior." In *Proceedings of the 3rd ACM conference on Electronic Commerce (EC '01).* Association for Computing Machinery, New York, NY, USA, 38–47. https://doi.org/10.1145/501158.501163.

Straub, Detmar, Mark Keil, and Walter Brenner. 1997. "Testing the Technology Acceptance Model across Cultures: A Three Country Study." *Information & Management* 33 (1): 1–11.

Stroshane, Eric. 2018. "More than a Week – 'Choose Privacy' Is Now an Everyday Choice." *Choose Privacy Every Day* (blog). June 19, 2018. https://chooseprivacyeveryday.org/more-than-a-week-choose-privacy-is-now-an-everyday-choice/.

Stepanova, Olga. 2018. "Germany." In *The Privacy, Data Protection and Cybersecurity Law Review*, edited by Alan Charles Raul, 146–53.

Story, Peter, Sebastian Zimmeck, and Norman Sadeh. 2018. "Which Apps Have Privacy Policies? An Analysis of over One Million Google Play Store Apps." Peter Story Sebastian Zimmeck Norman Sadeh. February 2018. http://reports-archive.adm.cs.cmu.edu/anon/isr2018/abstracts/18-100.html.

Stoyanov, Stoyan R., Leanne Hides, David J. Kavanagh, Oksana Zelenko, Dian Tjondronegoro, and Madhavan Mani. 2015. "Mobile App Rating Scale: A New Tool for Assessing the Quality of Health Mobile Apps." *JMIR MHealth and UHealth* 3 (1): e27. https://mhealth.jmir.org/2015/1/e27.

Strain, Matt. 2015. "1983 to Today: A History of Mobile Apps | Media Network | The Guardian." February 13, 2015. https://www.theguardian.com/media-network/2015/feb/13/history-mobile-apps-future-interactive-timeline.

Taddicken, Beate. 2014a. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure." *Journal of Computer-Mediated Communication* 19 (2): 248–73. https://doi.org/10.1111/jcc4.12052.

———. 2014b. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure." *Journal of Computer-Mediated Communication* 19 (2): 248–73. https://doi.org/10.1111/jcc4.12052.

Taneja, Aakash, Jennifer Vitrano, and Nicolas J. Gengo. 2014. "Rationality-Based Beliefs Affecting Individual's Attitude and Intention to Use Privacy Controls on Facebook: An Empirical Investigation." *Computers in Human Behavior* 38 (September): 159–73. https://doi.org/10.1016/j.chb.2014.05.027.

Taylor, Kyle, and Laura Silver. 2019. "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally." Pew Research Center 5. https://www.pewresearch.org/global/wp-content/uploads/sites/2/2019/02/Pew-Research-Center_Global-Technology-Use-2018_2019-02-05.pdf.

Tene, Omer, and Jules Polonetsky. 2013. "A Theory of Creepy: Technology, Privacy and Shifting Social Norms." Yale JL & Tech. 16: 59. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1098&context=yjolt.

The Economist. 2018. "America Should Borrow from Europe's Data-Privacy Law," April 5, 2018. https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

"The Results Are In..." Mozilla. Email. May 8, 2018.

Thurm, Scott, and Yukari Iwatani Kane. 2010. "Your Apps Are Watching You." *Wall Street Journal*, December 17, 2010, sec. Tech. https://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

Trepte, Sabine, and Philipp K. Masur. 2016. "Cultural Differences in Social Media Use, Privacy, and Self-Disclosure: Research Report on a Multicultural Study." http://opus.uni-hohenheim.de/volltexte/2016/1218/.

———. 2017. "Privacy Attitudes, Perceptions, and Behaviors of the German Population." https://doi.org/10.13140/RG.2.2.25818.95684.

Tully, S, and Y Mohanraj. 2017. "Mobile Security: A Practitioner's Perspective." In *Mobile Security and Privacy: Advances, Challenges and Future Research Directions*, 5–55. Elsevier.

Umlauf, Konrad, Simone Fühles-Ubach, and Michael S. Seadle, eds. 2013. *Handbuch Methoden Der Bibliotheks- Und Informationswissenschaft: Bibliotheks-, Benutzerforschung, Informationsanalyse*. Berlin: De Gruyter/Saur.

"Undergraduate Scholarly Habits Ethnography Project." n.d. Accessed October 3, 2018. https://ushep.commons.gc.cuny.edu/project-design/.

Urry, John. 2002. "Mobility and Proximity." *Sociology* 36 (2): 255–74. https://doi.org/10.1177/0038038502036002002.

"US State Comprehensive Privacy Law Comparison." n.d. Accessed October 11, 2019. https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

Van Kleek, Max, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, and Nigel Shadbolt. 2017. "Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps." In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 5208–20. Denver, Colorado, USA: ACM Press. https://doi.org/10.1145/3025453.3025556.

"VDB - Verein Deutscher Bibliothekarinnen Und Bibliothekare: Datenschutz: Grundlagen. Umsetzung Der EU-Datenschutzgrundverordnung in Deutschland." 2018. July 5, 2018. https://www.vdb-online.org/veranstaltung/794/.

Wang, Xiaolei, Yuexiang Yang, Chuan Tang, Yingzhi Zeng, and Jie He. 2016. "DroidContext: Identifying Malicious Mobile Privacy Leak Using Context." In EEE

Trustcom/BigDataSE/ISPA, Tianjin, 2016: 807–14. IEEE. https://doi.org/10.1109/TrustCom.2016.0142.

Ware, Willis H. 1977. "Computers and Personal Privacy." *Proceedings of the American Philosophical Society* 121 (5): 355–59.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193-220.

Warren, Tom. 2013. "Millions of Android Users 'deceived' by Flashlight App That Shares Location with Advertisers." The Verge. December 6, 2013. https://www.theverge.com/2013/12/6/5181472/brightest-flashlight-free-ftc-location-data-settlement.

Westin, Alan F. 1967. *Privacy and Freedom*. Vol. 1. Atheneum New York.

"Which Messenger Services Do You Use Regularly?" Chart. April 23, 2019. Statista. Accessed August 15, 2019. h." n.d. https://www.statista.com/forecasts/998694/messenger-usage-by-brand-in-germany.

Whitman, James Q. 2003. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale LJ* 113: 1151.

Wijesekera, Primal, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. "The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences." In *Security and Privacy (SP), 2017 IEEE Symposium On*, 1077–93. IEEE.

Yang, Esther, Jason Burger, Marcus Peters, Brandon Cruz, and Hannah Steinberg. 2016. "Customer Service Management & Hofstede's Cultural Dimensions In Australia, Brazil, China, Germany, Japan, Norway, And The Usa." In *Allied Academies International Conference. Academy of Organizational Culture, Communications and Conflict. Proceedings*, 21:62. Jordan Whitney Enterprises, Inc.

Yang, Zeyang, Kathryn Asbury, and Mark D. Griffiths. 2019. "Do Chinese and British University Students Use Smartphones Differently? A Cross-Cultural Mixed Methods Study." *International Journal of Mental Health and Addiction* 17 (3): 644–57. https://doi.org/10.1007/s11469-018-0024-4.

Ybarra, Laura. 2011. "The EU Model as an Adoptable Approach for US Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States." *Loy. LA Int'l & Comp. L. Rev* 34: 267.

Yerukhimovich, Arkady, Rebecca Balebako, Anne Boustead, Robert K Cunningham, William Welser IV, Richard Housley, Richard Shay, Chad Spensky, Karlyn D Stanley, and Jeffrey Stewart. 2016. "Can Smartphones and Privacy Coexist Assessing Technologies and Regulations Protecting Personal Data on Android and IOS Devices."

Massachusetts Institute of Technology-Lincoln Laboratory Lexington United States. https://apps.dtic.mil/sti/pdfs/AD1020293.pdf.

Young, Alyson Leigh, and Anabel Quan-Haase. 2013. "Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited." *Information, Communication & Society* 16 (4): 479–50. https://doi.org/10.1080/1369118X.2013.777757.

Zheng, Pei, and Lionel Ni. 2006a. *Smart Phone and Next-Generation Mobile Computing*. The Morgan Kaufmann Series in Networking. Amsterdam [u.a]: Elsevier/Morgan Kaufmann.

———. 2006b. "6 - Mobile Security and Privacy." In *Smart Phone and Next Generation Mobile Computing*, edited by Pei Zheng and Lionel Ni, 335–405. Burlington: Morgan Kaufmann. https://doi.org/10.1016/B978-012088560-2/50008-3.

Zimmer, Michael, and Bonnie Tijerina. 2018. "Library Values & Privacy in Our National Digital Strategies: Field Guides, Convenings, and Conversations,"1 –11. https://cpb-us-w2.wpmucdn.com/sites.uwm.edu/dist/b/524/files/2018/08/LibraryValuesAndPrivacy_Report-28qqhtp.pdf.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First edition. New York: Public Affairs.

Zuckerberg, Mark. 2019a. "A Privacy-Focused Vision for Social Networking | Facebook." March 6, 2019. https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

———. 2019b. "Facebook-Chef Mark Zuckerberg: Vier Ansätze zur Regulierung des Internets." *FAZ.NET*, March 30, 2019. https://www.faz.net/1.6115996.

———. 2020. "Starting the Decade by Giving You More Control Over Your Privacy." *About Facebook* (blog). January 28, 2020. https://about.fb.com/news/2020/01/data-privacy-day-2020/.

Appendix 1: Demographic Question (in German)

A. Demographische Fragen

1. Wie alt bist du?

2. Machst du gerade … ☐ ein Bachelor-Studium
   ☐ ein Master-Studium?

3. Machst du ein ☐ Fernstudium?
   ☐ Direkt-Studium?:

4. Hast du neben dem Studium auch einen Job/eine Arbeitsstelle?

   ☐ JA ☐ NEIN Falls ja, was?

   Wie viele Stunden arbeitest du neben dem Studium?

   ☐ Unter 5 Std/Woche ☐ 6-10 ☐ 11-20 ☐ mehr als 20 Std./Woche

5. Hattest du vor dem Studium bereits einen Job/eine Arbeitsstelle?

   Falls ja, in welchem Berufsfeld?

6. Hast du eine Ausbildung gemacht? ☐ JA ☐ NEIN

   Falls ja, welche?

Appendix 2: Demographic Question English

A. Demographic Questionnaire

1. How old are you?

2. Are you currently enrolled as a ☐ bachelor degree student?
   ☐ a master degree student?

3. Are you taking your classes ☐ online? ☐ in person? ☐ hybrid?

4. Besides being a student, are you also working?
   ☐ Yes ☐ No If Yes, what do you do?

   And how many hours a week are you employed?
   ☐ less than 5 hours/per week ☐ 6-10
   ☐ 11-20 ☐ more than 20 hours/per week

5. Before you enrolled at Rutgers, did you work and/or study something else?

B. Fragen zu deinem Mobiltelefon und zur Nutzung des Mobiltelefons

1. Was für ein Smartphone hast du?
2. Besitzt du auch ein Tablet? Benützt du beide gleichermaßen oder gibt es da Unterschiede in deinem Nutzen? Die restlichen meiner Fragen werden sich jetzt nur auf dein Smartphone beziehen.
3. Was für ein mobiles Betriebssystem hat dein Handy?
4. Wie lange besitzt du schon dein aktuelles Smartphone?
5. Warum hast du gerade dieses Smartphone gewählt?
6. Erinnere dich an den Tag, an dem du dein erstes eigenes Smartphone *gekauft*/*bekommen* hast. Wann war das? Was war das für ein Modell? Welche Gedanken/Gefühle hattest du in dem Moment?
7. Wie oft benutzt du dein Mobiltelefon durchschnittlich pro Stunde?
   Wie oft pro Tag?
   Hast du unter der Woche ein anderes Verhalten als am Wochenende?
8. Besitzt du einen Computer? Welches Modell? Was für ein Betriebssystem hat der?
9. Vergleiche mal die Zeit, die du am Computer verbringst, mit der Zeit, die du mit dem Mobiltelefon verbringst.
10. Was machst du alles mit deinem Mobiltelefon? Erzähl mal ein bisschen ...
    Was machst du besonders häufig? Was eher selten?
11. Welche fünf Apps benutzt du sehr oft? Und warum?
    Erzähl mal ein bisschen von den Apps …
12. Unter den fünf Apps, welche ist deine absolute wichtigste, also deine Lieblings-App? Warum?
13. Würdest du dein Mobiltelefon einem Freund oder einem Familienmitglied für eine gewisse Zeit ausleihen? Wie lange? Würdest du es einer fremden Person ausleihen? Auch ohne zu sehen, was er/sie damit macht?

B. Question about your smartphone and how you use it

1. What kind of smartphone/phone do you have?
2. Do you also own a tablet? Looking at usage of your phone and tablet – would you say that there is a difference in how and for what you use your tablet? This is actually my only question about tablets. The rest of the interview will focus only on phone.
3. Do you know the operating system of your phone? Like the mobile operation system?
4. How long have you owned current phone?
5. Is there a reason why you choose this particular model or phone? Or Why did you choose this phone?
6. Now looking back a bit – do you remember the day or the time period when you bought or got your first smartphone? How many years ago was that?
   Do you remember the model or what kind of phone it was? Do you remember what your thoughts were and/or how it felt about it? What did you think about the new phone? How did you feel?
7. How many times per hour do you use your phone? Like on average? How many times a day? Would you say your usage behavior is different on weekends?
8. Do you own a computer? What kind? What operating system does it have?
9. If you compare your phone usage versus your computer usage do think there is a difference (for example if you would give me a percentage).
10. What do you do with your phone? Can you tell me a bit about your phone usage habits? What do you use it for? What are things you use it for a lot and what are things you rarely do with it?
11. What apps do you use the most? Can you give me your top five? Can you tell me a bit about those five apps and what you use them for?
12. You just told me your five top apps, which one would you say is your absolute number 1? Your most favorite app? Or the one you use the most? Why?
13. Would you lend your phone to a friend or family member? If so for how long?
    Would you lend your phone to a person you just met, like a stranger? Would the stranger be allowed to use the phone without you seeing what he or she is actually doing on your phone?

C. Experiment und Beobachtung

14. Kannst du mir an deinem Telefon mal zeigen, ob es oder wo es Einstellungen gibt, um deine Daten und persönlichen Informationen zu schützen?

15. Nun würde ich dich bitten, eine von mir ausgewählte App an deinem Telefon herunterzuladen und zu installieren.
    Dazu vorab zwei Bemerkungen:
    Natürlich kannst du diese App sofort nach dem Interview wieder entfernen.
    Wenn du die App nicht an deinem eigenen Mobiltelefon installieren willst, kannst du auch gerne mein Mobiltelefon dafür benutzen. Ich kann dir mein Android oder iPhone geben.
    Hier ist der Name einer App: **Perfect Piano** *(auf einem Zettel ist der Name der App gut lesbar)* Erzähle einfach mal so ein bisschen wie du das normalerweise machst.

16. Vorhin hast du gesagt, dass das [*Name der genannten App*] deine Lieblings-App ist. Kannst du sie mir mal auf deinem Mobiltelefon zeigen? Was für Zugriffe hat diese App auf deine persönlichen Informationen und Daten? Kannst Du mal die Datenschutzrichtlinie für diese App suchen ...

17. Benutzt du WhatsApp? Falls nein, warum nicht.
    Falls ja, …
    WhatsApp war ja vor einiger Zeit sehr im Gespräch.
    Weißt du, worum es da ging? Kannst du dich an irgendwas erinnern?

C. Experiment and observation

14. Let's look at your phone now. Do you know where the privacy settings on your phone are? **Like settings to protect your personal data/and or information?** Can you show it to me?
15. I am going to ask you now to download an app onto your phone. I would like to tell you two things beforehand 1) You can delete and uninstall the app immediately after the interview is over and 2) If you don't want to use your personal phone I can give you either my Android phone or my iPhone.
    Okay – so that's the app (give note with name of app to student): Perfect Piano. So just download it and tell me a bit about how you usually do that.
16. You told me that [name of app] is the one you use the most. Can you show it to me on your phone? Do you know what personal information/data and personal content this app has access too? Do you know where the privacy policy of this app is? Can you show it to me?
17. Do use WhatsApp? If not why?
    If yes can you tell me anything about?

Appendix 7:
Questions about mobile data privacy/data protection and mobile privacy (in German)

D. Fragen zum mobilen Datenschutz und zur Privatsphäre *(nach dem Experiment)*

18. Jetzt kommen ein paar allgemeine Fragen.
    Denk mal kurz darüber nach, was Privatsphäre für dich bedeutet.

19. Wir kommen zu einem anderen Begriff: Datenschutz
    Was meinst du?

20. Ich gebe dir jetzt gleich zwei Begriffe zum Nachdenken. Meine Fragen dazu sind:

    - Welche Assoziationen hast du zu den beiden Begriffen?
    - Welche Bedeutung haben diese Begriffe für dich?

    Hier ist Begriff 1: Privatsphäre auf meinen Mobilgeräten
    Und hier Begriff 2: Datenschutz auf meinen Mobilgeräten

21. Was glaubst du, was für persönliche Daten und Informationen von deinem Mobiltelefon mit „anderen" geteilt werden? Und wer sind denn diese „anderen", die an deine Daten und Informationen kommen? Kannst du mal ein paar aufzählen?
    Was denkst du passiert mit all den gesammelten Daten? Wer hat daran Interesse? Warum? Zu welchem Zweck?

22. Ein kleiner Blick in die Zukunft:
    Glaubst du eigentlich, dass persönliche Daten und Informationen geschützt werden sollten? Oder bist du eher der Ansicht, dass deine Daten transparent sein dürfen/müssen?
    Und dass damit auch du transparent für alle bist sozusagen der gläserne Mensch für alle?

    Changed to: Jetzt mal so eine abschließende Frage – also, wie ist es denn: Findest du es okay, dass unsere ganze Informationen, also unsere persönliche Informationen auf diesen mobilen Geräten eben transparent sind, dass wir so ein bisschen so dieser gläsernen Mensch werden, also macht nichts ist okay, ich teile alles, jeder kann alles von mir wissen, oder bist du eher so ne, ich denke mal, dass muss sich ändern?

    Würdest du jetzt sagen, wenn es die Möglichkeit gebe, dass eine Firma dir Datenschutz und mobile Privatsphäre garantiert, würdest du es machen?

D. Questions about mobile data privacy/data protection and mobile privacy

18. I am going to ask you some more general questions now:
    Can you tell me what privacy is or what privacy means to you?

19. What about data protection?

20. I am going you to give you now 2 concepts and I would like you to tell me what they mean to you – just think a bit about it – or brainstorm a bit …
    - just think a bit about it – or brainstorm a bit …

    The first word is mobile privacy?
    And the second word is mobile data protection?

21. Can you think for a little bit about the next question …
    What personal information and data from your phone is actually being shared with "Others" And who are these "Others" or let say players or stakeholders that can maybe access it? What do you think happens with all the collected information/data? Who is interested in it? Why? And for which purpose?

22. Okay – you made it – this is the final question.
    So … is it actually okay with you that all our personal information or data that we have on our smartphones is transparent? Like is it okay for you let's say that you and I or we as people as humankind and all our information and personal data is transparent? As if we made out of glass … Like I don't care, I don't mind sharing everything and everybody can know everything about me …
    Or do you actually think that this is not good and things should or need to change?

Appendix 9: Research Approval Letter *(page 1 of 2)*

Stefanie Havelka
[redacted]

Professor Dr. Michael Seadle
Geschäftsführender Institutsdirektor
und Prodekan der Philosophischen Fakultät I
Institut für Bibliotheks- und Informationswissenschaft
Unter den Linden 6
10099 Berlin
Germany

Nov 2018
Re: Approval to conduct research with human subjects

Dear Professor Dr. Seadle,

I hereby officially request approval to conduct research with human subjects as part of my dissertation.

My dissertation investigates digital privacy as it relates to user behavior and attitude on mobile devices. More specifically, I will examine how users' understanding of mobile privacy differs from culture to culture.

Research will be conducted with two different sets of human subjects. The first set will be comprised of ten students from the Master Program/Distance Learning in Library and Information Science at the Berlin School of Library and Information Science, Humboldt University in Berlin. The second set will be made up of ten students enrolled in the Master of Information Program concentrating in Library and Information Science at Rutgers University, New Brunswick, New Jersey, USA. Participation is voluntary, and subjects may leave the study at any time without prejudice or penalty.

All subjects will be asked to sign a fully informed consent agreement at the begin of the study. Data will be collected via in-person interviews and an experiment that includes participant observation. Data will be audio and/or video recorded. All data will be anonymized and only I will have access to the recordings/transcripts. I will protect confidentiality by securely storing the data on my password-protected computer.

In conclusion, I would like to emphasize that this study involves minimal risk to participants. The probability of harm or discomfort to be incurred during in the research is no greater that encountered in daily life. While the intent is to publish the results of the study, the identity of each participant will remain anonymous in all published materials.

Please don't hesitate to contact me if you have any further questions.

Sincerely,

Stefanie Havelka

New York, NY, USA, November 5, 2016

Appendix 10: Research Study Invitation (in German)

EINLADUNG zur Teilnahme an einer Studie Nov 2016

Betreff: GESUCHT Interview-Teilnehmer / -innen für meine Doktorarbeit zum Thema *Mobiler Datenschutz, Privatsphäre und Apps*
Die Aufwandsentschädigung für die Teilnahme beträgt **10 €.**

Liebe Studentinnen und Studenten,

im Rahmen meiner Doktorarbeit zum Thema *Mobiler Datenschutz, Privatsphäre und Apps* untersuche ich die Einstellung und das Verhalten deutschen und amerikanischen Bibliotheks- und Informationswissenschaft Student/innen in Bezug auf Datenschutz, Privatsphäre und mobilen Apps am Smartphone und/oder Tablet.

Hierfür suche ich Interview-Teilnehmer / -innen.
Die Dauer des Interviews beträgt ungefähr 45 – 60 Minuten und wird mit dem Einverständnis des Teilnehmers / der Teilnehmerin als Audio und/oder Video aufgezeichnet. Zu Beginn der Studie werden alle Teilnehmer / -innen detailliert über den Inhalt und Zweck des Interviews informiert.

Die Studienteilnahme ist mit keinerlei gesundheitlichen Risiken verbunden. Jedoch werden Ihnen während des Interviews persönliche Fragen gestellt werden.
Für Ihre Teilnahme erhalten Sie am Ende des Interviews eine symbolische Aufwandsentschädigung von **10 €.**

Alle in dieser Studie gesammelten Daten werden anonymisiert ausgewertet und ausschließlich von mir für den Zweck meiner Doktorarbeit verwendet. Ihre Daten und ggf. die Video-Aufnahme wird vertraulich und durch ein Passwort geschützt sicher aufbewahrt. Ausschließlich ich, Stefanie Havelka, habe Zugang zu den Daten. Alle Ergebnisse der Studie werden anonymisiert und ohne Bezug auf konkrete Personen wissenschaftlich veröffentlicht.

Die Teilnahme an dieser Studie ist freiwillig. Teilnehmer/-innen haben jederzeit die Möglichkeit, die Studie ohne Angabe von Gründen abzubrechen. Die Einwilligung zur Verwendung Ihrer Daten können Sie während der Teilnahme an der Studie jederzeit widerrufen.

Alle Teilnehmer dieser Studie erhalten zu Beginn des Interviews eine Kopie ihrer Einverständniserklärung für Ihre Unterlagen.

Wenn Sie Interesse haben, dann schreiben Sie bitte ein E-Mail an: Stefanie Havelka [redacted]

Für weitere Informationen oder bei Fragen stehe ich Ihnen gerne per E-Mail zur Verfügung.
Für Ihr Interesse bedanke ich mich im Voraus.

Mit den besten Grüßen aus New York City

Stefanie Havelka
Assistant Professor
Web and Mobile Services Librarian
Leonard Lief Library, Lehman College, CUNY

February 2017

Invitation to participate in doctoral research study

Subject: Interview participants needed to participate in a doctoral research study on mobile privacy/data security. Receive $15 as a participation reward!

Dear Rutgers students,

Your help is needed: Please participate in my doctoral research study!

My dissertation investigates privacy as it relates to user behavior and attitudes on mobile devices and apps. I will examine how users' understanding of mobile privacy differs from culture to culture, using ethnographic methodologies to measure differences in attitudes between U.S. and German library and/or information science students.

Each interview will last approximately 45-60 minutes. Participation is voluntary, and subjects may leave the study at any time without prejudice or penalty. All subjects will be asked to sign a fully informed consent agreement at the beginning of the interview. If participants consent, the interviews will be audio and/or video recorded. Participants will also receive a copy of the signed consent form.

This study involves minimal risk to participants. However, participants will be asked personal questions in regard to the research subject. The probability of harm or discomfort to be incurred during in the research is no greater than that encountered in daily life. **All participants will receive $15 for their time.**

All data will be anonymized and only I will have access to the recordings/transcripts. I will protect the collected data confidentiality by securely storing it on my password-protected computer. While the intent is to publish the results of the study, the identity of each participant will remain anonymous in all published materials.

If you are interested, or have further questions, please contact me at:

Stefanie Havelka
[redacted]

Thank you for your time, support and interest.

Sincerely,

Stefanie Havelka
Assistant Professor
Web and Mobile Services Librarian
Leonard Lief Library, Lehman College, CUNY

Humboldt-Universität zu Berlin | Institut für Bibliotheks- und Informationswissenschaft
Unter den Linden 6 | 10099 Berlin | Deutschland

Stefanie Havelka | Doktorandin | [redacted]
9. Januar 2017

Einverständniserklärung

Sehr geehrte Probandin, sehr geehrter Proband,

vielen Dank für Ihre Teilnahme an diesem Interview.

Im Rahmen meiner **Doktorarbeit**

zum Thema ***Mobiler Datenschutz, Privatsphäre und Apps***

untersuche ich, Stefanie Havelka, die Einstellung und das Verhalten von deutschen und amerikanischen Bibliotheks- und Informationswissenschaft Student/innen in Bezug auf Datenschutz, Privatsphäre und mobilen Apps am Smartphone und/oder Tablet.

Die Dauer des Interviews beträgt insgesamt circa 45 – 60 Minuten und besteht aus drei Teilen.

Sie profitieren von der Teilnahme an diesem Interview insofern, als dass Sie sich mehr Gedanken über mobilen Datenschutz und Privatsphäre an Ihren mobilen Endgeräten machen und eventuell darauf reagieren oder natürlich auch nicht.

Mit Ihrem Einverständnis werde ich das Interview als Audio aufnehmen.
Der experimentelle Teil des Interviews wird außerdem als Video aufgezeichnet

Die Studienteilnahme ist mit keinerlei gesundheitlichen Risiken verbunden.
Jedoch werden Ihnen während des Interviews persönliche Fragen gestellt werden.

Für Ihre Teilnahme erhalten Sie am Ende der Untersuchung eine symbolische Aufwandsentschädigung von **10 €**.

Alle in dieser Studie gesammelten Daten werden anonymisiert ausschließlich von mir ausgewertet und im Rahmen meiner Doktorarbeit verwendet.

Alle Ergebnisse der Studie werden anonymisiert und ohne Bezug auf konkrete Personen wissenschaftlich in Form einer Doktorarbeit veröffentlicht.

Ihre Daten sowie ggf. die Video-Aufnahme werden vertraulich und durch ein Passwort geschützt sicher aufbewahrt. Ausschließlich ich, Stefanie Havelka, habe Zugang zu den Daten.

Ihre Teilnahme an dieser Studie ist freiwillig. Sie haben jederzeit die Möglichkeit, die Studie ohne Angabe von Gründen abzubrechen. Die Einwilligung zur Verwendung Ihrer Daten können Sie während der Teilnahme an der Studie jederzeit widerrufen.

Humboldt-Universität zu Berlin | Institut für Bibliotheks- und Informationswissenschaft
Unter den Linden 6 | 10099 Berlin | Deutschland

Stefanie Havelka | Doktorandin | [redacted]

Als Teilnehmer dieser Studie erhalten Sie eine Kopie dieser Einverständniserklärung für Ihre Unterlagen.

☐ Ich habe die aufgeführten Bedingungen gelesen und verstanden. Eventuelle Fragen sind durch die Doktorandin, Stefanie Havelka ausreichend beantwortet worden. Ich hatte genügend Zeit, eine Entscheidung zu treffen. Mit meiner Unterschrift bestätige ich mein Einverständnis zur Teilnahme an dieser Studie.

Name (in Druckschrift):

_____

Datum:

_____

Unterschrift:

_____

Unterschrift Doktorandin, Stefanie Havelka:

_____

March 4, 2017

Consent to Participate in Research

Dear Student,

Thank you for participating in my doctoral research study.

Procedure: My dissertation investigates privacy as it relates to user behavior and attitudes on mobile devices and apps. More specifically, I, Stefanie Havelka, will examine how users' understanding of mobile privacy differs between United States and German library and/or information science students.

The interview will ~~be~~ last approximately 45 – 60 minutes. The interview will be in three parts: 1) questions about your smartphone usage 2) a practical experimental part and 3) general questions on privacy and personal data protection in relation to mobile devices.

With your permission, I will videotape and take notes during the interview. The recording is to accurately document the information you provide, and will be used for transcription purposes only. If you agree to being videotaped, but feel uncomfortable at any time during the interview, I can turn off the recorder at your request.

Benefits: Participating in the study may help you gain a better understanding about mobile data protection and mobile privacy.

Possible Discomforts and Risks: This study involves minimal risk. However, you will be asked personal questions in regard to the research subject. The probability of harm or discomfort incurred during the research is no greater than that encountered in daily life.

Voluntary Participation: Your participation in this study is voluntary, and you may decide not to participate without prejudice, penalty, or loss of benefits to which you are otherwise entitled. You may leave the study at any time.

Confidentiality
All data will be anonymized and only I, Stefanie Havelka will have access to the recordings/transcripts. I will protect the collected data confidentiality by securely storing it on my password-protected computer. While the intent is to publish the results of the study, the identity of each participant will remain anonymous in all published materials.

Compensation: To thank you for participating in this study, you will receive $15 US Dollars in cash.

Humboldt-Universität zu Berlin | Berlin School of Information and Library Science
Unter den Linden 6 | 10099 Berlin | Germany

Stefanie Havelka | doctoral student [redacted]

Consent:

You will be given a copy of this consent form to keep for your own records.

I have explained the study to

_____ (name of participant)

in a language he/she understands, and he/she has agreed to be in the study.

If you wish to participate in this study, please sign and date below.

_____
Participant's Name (please print)

_____ _____
Participant's Signature Date

_____ _____
Signature of doctoral student Date

Appendix 14: Interview Transcription Guidelines

Based on Qualitative Text Analysis book by Udo Kuckartz (2014). Page 124-127, and Dresing, Thorsten / Pehl, Thorsten / Schmieder, Christian (2015): Manual (on) Transcription. Transcription Conventions, Software Guides and Practical Hints for Qualitative Researchers. Page 28-32

1. Transcribe literally; do not summarize or transcribe phonetically. Dialects are to be accurately translated into standard language. If there is no suitable translation for a word or expression, the dialect is retained.
2. Informal contractions are not to be transcribed, but approximated to written standard language. E. g. "gonna" becomes "going to" in the transcript. Sentence structure is retained despite possible syntactic errors.
3. Discontinuations of words or sentences as well as stutters are omitted; word doublings are only transcribed if they are used for emphasis ("This is very, very important to me.") Half sentences are recorded and indicated by a slash /.
4. Punctuation is smoothed in favor of legibility. Thus, short drops of voice or ambiguous intonations are preferably indicated by periods rather than commas. Units of meaning have to remain intact.
5. Pauses are indicated by suspension marks in parentheses (...).
6. Affirmative utterances by the interviewer and interviewee, like "uh-huh, yes, right" etc. and monosyllabic answers are always transcribed. Add an interpretation, e.g. "Mhm (yes)" or "Mhm (no)".
7. Words with a special emphasis are CAPITALIZED.
8. Any disruption should be listed specifically (e.g. phone rings)
9. Every contribution by a speaker receives its own paragraph. In between speakers there is a blank line. Short interjections also get their own paragraph.
10. Emotional non-verbal utterances of all parties involved that support or elucidate statements (laughter, sighs) are transcribed in brackets. Disturbance and other comments and remarks are also put in brackets.
11. Symbols and abbreviations such as percent and meter etc. are spelled out.
12. Contractions and short forms are transcribed exactly as they are spoken, e.g. ‘can’t’ instead of ‘cannot’ or ‘stats’ instead of ‘statistics’
13. Concerning capitalization, words in different languages are spelled according to the rules of the English language.
14. If direct speech is quoted in a recording, the quote is put in quotation marks: and then I said "Well, let’s see about that."
15. Numbers are transcribed as follows:
    a. Zero to twelve are spelled out, larger numbers are transcribed as numerals.
    b. Numbers that make short words are also spelled out, especially round numbers: twenty, hundred, three thousand.
16. Proper names are capitalized e.g. Facebook, Instagram etc.
17. Discontinuations are marked by /: "I was worri/ concerned." Word doublings are always transcribed.

Appendix 15: Final deductive categories Phase 4: Fieldwork 1

Final deductive priori categories
mobile privacy
mobile privacy attitude
mobile privacy behavior
app experiment Perfect Piano
app experiment favorite app
transparent human
app experiment privacy
personal information and data shared
mobile privacy definition
mobile data protection definition
WhatsApp
lend mobile phone family friend
lend mobile phone stranger
mobile security
mobile phone habit
daily usage
computer versus phone usage
top five apps
favorite app
mobile phone attitude
first smartphone
mobile phone knowledge
privacy definition
data protection definition

Appendix 16:
Final inductive categories with corresponding deductive category. Phase 5: Fieldwork 1

main deductive categories	inductive subcategories
mobile phone attitude	Android iPhone Other
mobile phone attitude	value for money
lend mobile phone stranger	value
lend mobile phone stranger	theft
lend mobile phone stranger	security risk
lend mobile phone stranger	personal information
lend mobile phone family friend	personal device
lend mobile phone family friend	breakage
app experiment privacy	location service
app experiment Perfect Piano	reviews stars pictures
app experiment Perfect Piano	privacy policy
mobile phone habit	phone calls
mobile privacy attitude	expressions/words/ phrases/ non-verbal cues
mobile privacy attitude	data as trade
mobile privacy attitude	convenience laziness
mobile privacy attitude	complacency/learned helplessness
mobile privacy attitude	confusion/unclear
mobile privacy attitude	Google/Facebook/ Amazon/Apple
mobile privacy attitude	awareness/education
mobile privacy attitude	abstractness
mobile privacy attitude	law/regulation/control
mobile privacy attitude	ethical/moral/ philosophical/ societal
mobile privacy attitude	privacy policy
mobile privacy attitude	surveillance
mobile privacy attitude	advertising